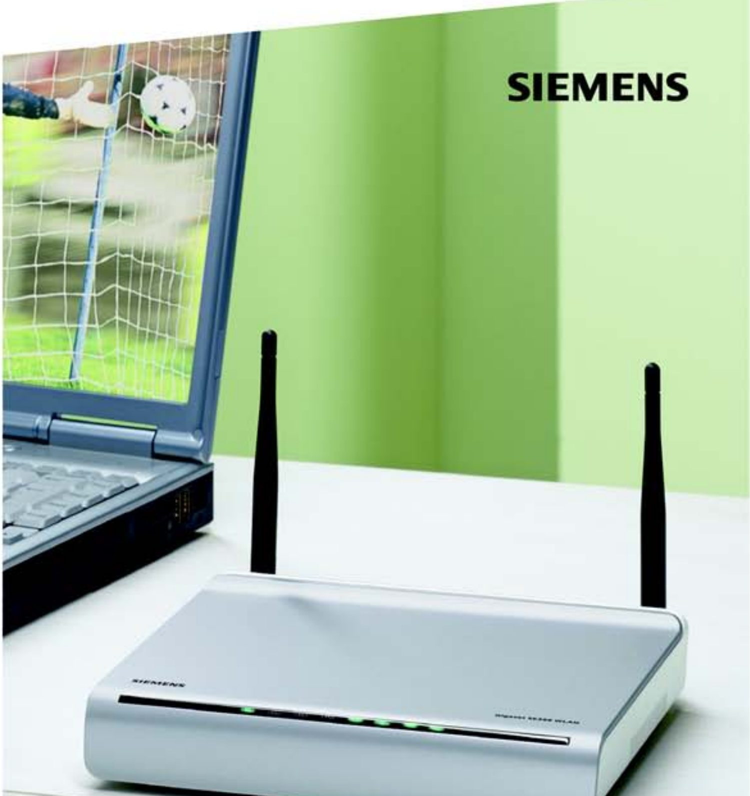
SIEMENS



Gigaset
SE366 WLAN

XSPAN™ ATHEROS

Contents

##

##

Safety precautions

- Only use the mains adapter that is supplied with the device.
- The device is only intended for operation in enclosed rooms (temperature range: 0 to 40°C). Do not use the device in a damp or wet environment, with dust or vapours.
- Only connect the device via LAN cabling which runs exclusively in enclosed rooms.
- The device may affect medical equipment.
- Make sure you include the operating instructions and the CD-ROM when you pass on your device to somebody else.

Your contribution to the environment (ECO)

We at Gigaset Communications GmbH make our products as environmentally compatible as possible. Our goal is a sustainable process that makes it easier for us to comply with the strict stipulations of the ISO standard 14001 for international environmental management.

Further advantages for the ecology

- Thanks to a switched-mode power supply, all our routers and repeaters use up to 60% less power and so offer higher energy efficiency.
- You can reduce the WLAN's transmitting power for all routers and repeaters and some WLAN clients – depending on the device in question and your PC's operating system.
- You can turn off the WLAN completely.

Trademarks

Gigaset Communications GmbH is a trademark licensee of Siemens AG.

Microsoft, Windows Vista, Windows XP, Windows 2000 and Internet Explorer are registered trademarks of Microsoft Corporation.

Mozilla Firefox is a registered trademark of the Mozilla Organization.

The Gigaset SE366 WLAN

Your Gigaset SE366 WLAN is a powerful but easy-to-use device that connects your PC (WLAN) or your local network (LAN) to the Internet without the need for wires (via a DSL or cable modem).

You can connect your PC wirelessly to the Gigaset SE366 WLAN and create a wireless local network (WLAN). For network security, wireless transmission can be encrypted using the WPA standard or 64/128-bit WEP.

The Gigaset SE366 WLAN allows several users to access the Internet simultaneously. A single user account can be shared, if your Internet Provider permits this. If you want to surf the Internet at the lowest possible cost, then the Gigaset SE366 WLAN is a convenient and effective solution.

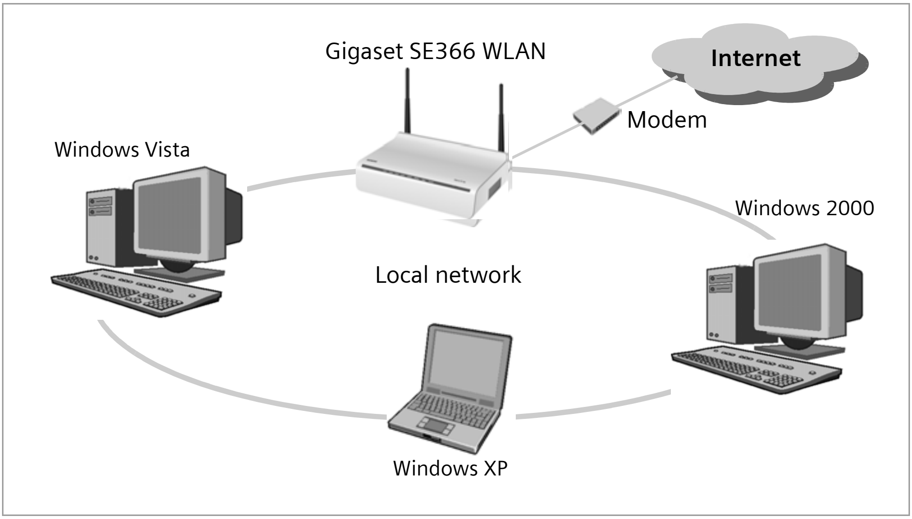
You can connect a DSL or cable modem to the WAN interface of your Gigaset SE366 WLAN.

Despite its extensive range of functions, the Gigaset SE366 WLAN is easy for both experts and non experts to handle. It can be configured and made operational within a few minutes.

The Gigaset SE366 WLAN provides the new WPS function for wireless connections of PCs or notebooks. You can activate this function with the registration button. If the other clients in your wireless network, such as the Gigaset PC Card 300, also support WPS, you can connect with one click only.

Local networks with Gigaset products

You can use the Gigaset SE366 WLAN to set up a local area network, e.g. a home network. All the PCs in this network can communicate with each other and have access to the Internet.



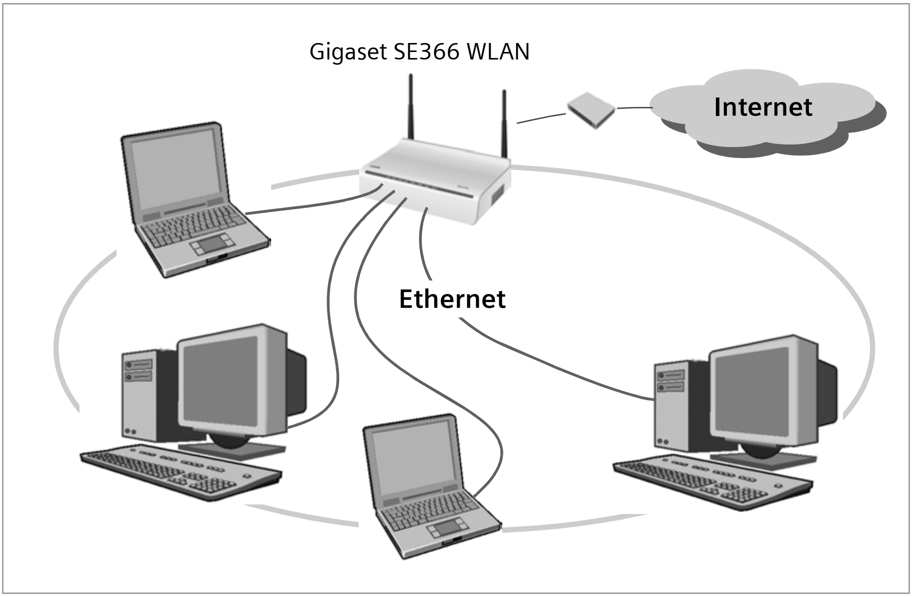
There are various ways in which you can set up the network with a Gigaset SE366 WLAN. You can

- set up a wired local area network (Ethernet) and allow the connected PCs access to the Internet (see page 9),
- set up a wireless local network (WLAN) and allow the connected PCs access to the Internet (see page 10),
- set up a local network comprising wireless and wired network components (see page 12).

Wired local area network (Ethernet)

In a wired local area network, PCs communicate with one another via an Ethernet cable. The Gigaset SE366 WLAN establishes the connection between the PCs, which you can connect to the four Ethernet LAN ports. The PCs must be equipped with a network socket (Ethernet). New PCs frequently already have this socket. For older PCs you will need to install an Ethernet network card. An Ethernet cable is used to connect the PC to the Ethernet LAN socket on the Gigaset SE366 WLAN. One cable is supplied with the device; you can obtain additional Ethernet cables from your retailer.

The Gigaset SE366 WLAN allows all PCs to access the Internet simultaneously.



Wireless local area network (WLAN)

In a wireless local area network (WLAN), PCs are linked without wires or cables. For this, the PCs have to be equipped with a wireless network adapter (WLAN adapter) such as a Gigaset PC Card 300 or a Gigaset USB Adapter 300.

We generally differentiate between two types of wireless network:

- Infrastructure mode
- Ad-hoc mode

Infrastructure mode

Infrastructure mode connects wireless and wired networks with one another. In addition to the mobile stations, infrastructure mode needs an access point such as the Gigaset SE366 WLAN. In infrastructure mode, the stations in the network always communicate via this access point. Each station that wants to be part of a wireless network must first be registered with the access point before it can exchange data.

The access point establishes the connection between the mobile stations of a wireless network and a wired LAN (Ethernet) or the Internet. This is described as the device's router functionality. The router sends data packets that are not addressed to stations within the network "outside," and forwards data packets originating from "outside" to the appropriate station within the network.

You can use the Gigaset SE366 WLAN to connect

- wirelessly networked PCs to the Internet and
- wirelessly networked PCs to an Ethernet network.

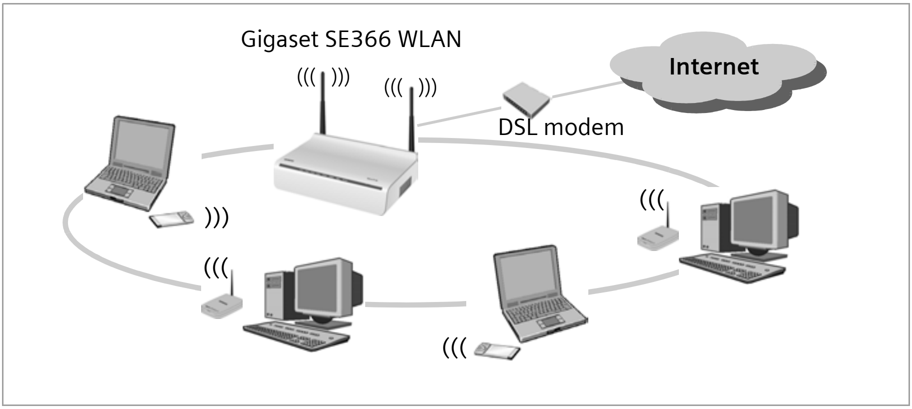
Infrastructure mode is the default configuration of the Gigaset SE366 WLAN. This configuration is described in the quick start guide that comes with the device.

Ad-hoc mode

An ad-hoc network is a wireless network that has been configured without an access point or a router. The mobile network components communicate with each other directly and wirelessly form the network on an "ad-hoc" basis, i.e. as and when required. All the stations in the network have the same rights. Ad-hoc networks are used wherever communications networks have to be set up quickly and without any existing network infrastructure, and where participants are on the move.

Linking wireless networks with the Internet

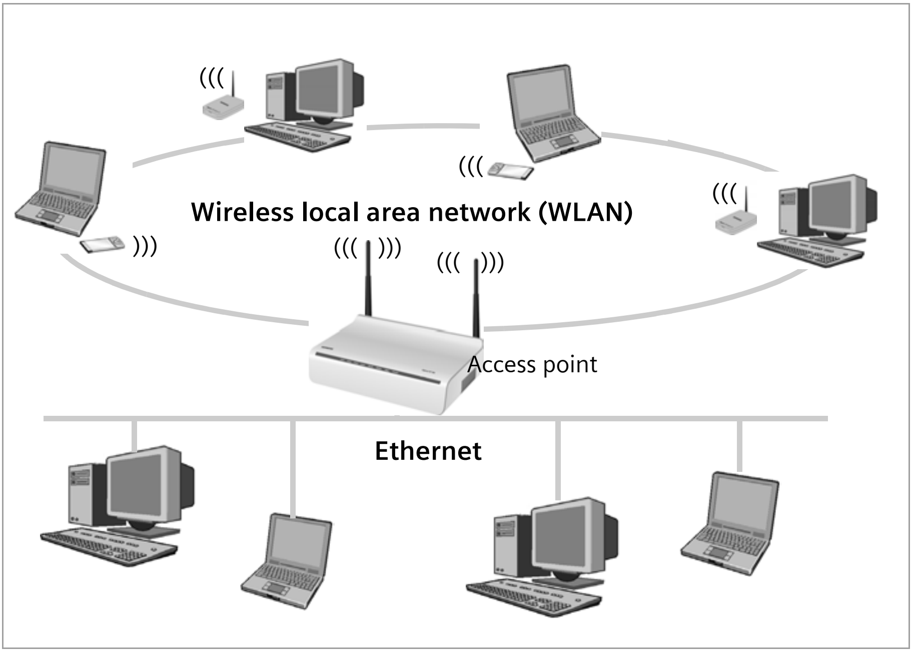
The Gigaset SE366 WLAN has a WAN port that permits all stations within its local area network to access the Internet simultaneously. To be able to use this functionality, you need a DSL or cable connection and a suitable modem. You can usually obtain the line and a modem from an Internet service provider.



This illustration shows the commonest method of application. One or more PCs communicate wirelessly with the Gigaset SE366 WLAN in infrastructure mode. The Gigaset SE366 WLAN forwards the data to the Internet via a DSL or cable modem. Data from the Internet flows back to the PC along the same route.

Linking a wireless network (WLAN) to an Ethernet (LAN)

Wireless local area networks can work easily together with existing Ethernet networks. If you wish to connect mobile stations to an existing wired network, you must group all the mobile stations into a wireless network in infrastructure mode.



The Gigaset SE366 WLAN has four Ethernet interfaces (LAN ports). Up to four PCs can be connected directly to these LAN ports.

All PCs can access the Internet via the Gigaset SE366 WLAN.

Note:

You can also connect an Ethernet router to a LAN port to access a larger Ethernet. If you want to link the Gigaset WLAN network to an existing network, a large number of settings have to be applied. It is therefore not possible for us to provide a general example for this use; configuration must be defined separately for each individual case. We advise having such networks configured by a specialist.

Security functions

You can use various encryption methods and authentication methods (WPA/WPA2-PSK,WPA/WPA2, WEP, MAC access control) to prevent unauthorised access to your wireless LAN or to make data illegible to unauthorised parties. The security settings available to you depend on the the components used in your local network. For detailed information, please consult the section "Setting security functions for the wireless network" on page 38.

WPS

Wifi-Protected-Setup (WPS) makes it easier to establish and encrypt a wireless network (1 click only). You no longer need to configure and synchronise the individual components of your wireless network manually.

A wireless network has a name (SSID) and requires the encryption of data traffic to protect against the risk of eavesdropping. The access point requires authentication with an SSID and - if encryption is activated - a key to allow a WLAN adapter to access the services.

WPS uses the encryption method WPA-PSK or WPA2-PSK. Devices with WPS automatically create an SSID and a WPA encryption key (pre-shared key) and synchronise each other.

WPS is not possible in networks using WEP encryption or WPA2/WPA authentication.

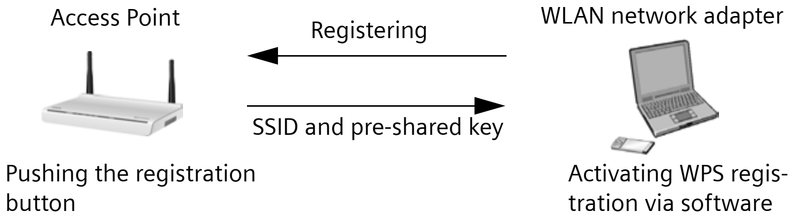
WPS provides two possibilities for registration:

- **Via registration button**

  The access point (e.g. the Gigaset SE366 WLAN) has a **WPS** button, while Gigaset devices have a button on the device’s back panel labelled **Registration**. After pushing this button, the device is ready to register a WLAN client (repeater or wireless network adapter) for two minutes.

  The first time this button is pushed, the device automatically creates an SSID and a pre-shared key. If a client activates its WPS registration within these two minutes, the security data is interchanged and a connection is established. It is ensured that only **one** client is allowed to synchronise within the two minutes.

Registering a PC


Access Point
Registering
WLAN network adapter
SSID and pre-shared key
Pushing the registration button
Activating WPS registration via software

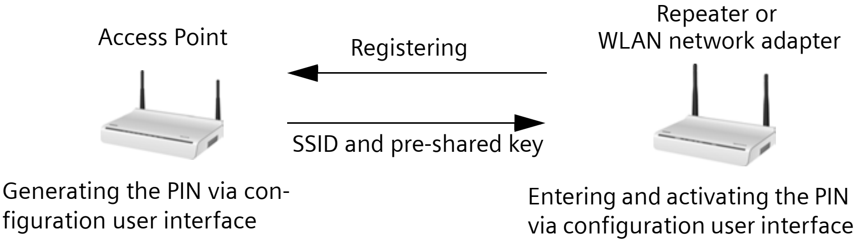
This procedure corresponds to the registration mode ***Push Button*** (default) on your Gigaset SE366 WLAN.

Please note that a new SSID and pre-shared key will be generated when the registration button is pushed for the first time after each factory reset of the Gigaset SE366 WLAN. This means that the clients have to be registered again.

◆ Via Personal Identification Number (PIN)

The PIN offers higher security for registration. No other device (e.g. of the neighbour) can log in unnoticed. A PIN is generated on one WLAN device, usually the access point, which has to be entered on the other devices for registration. If a client logs in with this PIN, the security data is synchronised.

It is also possible to create the PIN on one of the clients.


Access Point
Registering
Repeater or WLAN network adapter
SSID and pre-shared key
Generating the PIN via configuration user interface
Entering and activating the PIN via configuration user interface

If the PIN of the device that you are just configuring is to be used in your network, choose the registration mode ***Send own PIN***.

However, if the device is to use the PIN of another device, choose the registration mode ***Enter partner device PIN***.

WLAN adapters without WPS can also be set up manually, i.e. SSID and key must be entered manually. WPA-PSK encryption must be used.

Features and applications

The Gigaset SE366 WLAN's wide range of features make it ideal for a large number of applications, e.g.:

- **Internet access**

  The Gigaset SE366 WLAN gives several users access to the Internet when a DSL or cable modem is connected.

  - As many DSL providers set up Internet access via the PPPoE protocol, the Gigaset SE366 WLAN contains an integrated PPPoE Client, which means you no longer need to set up this service on your PC yourself.
  - Shared Internet access

    If your Internet provider permits this, the Gigaset SE366 WLAN supports Internet access for up to 252 users. In practice, multiple users in your network can surf the Internet simultaneously using just one Internet access.

- IP TV streaming

  The Gigaset SE366 WLAN allows the wireless transmission of IP TV (Internet television) to your IP TV receiver.

  Note:

  Please be aware, however, that video streaming may be disrupted depending on the following factors:

  - Removal of the wireless communication partner
  - Building substance (walls, power supply lines and water pipes)
  - Other sources of interference (other WLAN devices, Bluetooth, microwave, ...).

- **Setting up a local network**

  The Gigaset SE366 WLAN permits connections

  - for four devices via Ethernet ports with a transmission speed of 10 or 100 Mbps (with automatic recognition).
  - for up to 32 mobile terminals via a radio interface with a transmission speed of up to 300 Mbps. It complies with the IEEE 802.11n standard (draft, see note below) and can work with all products that satisfy the IEEE 802.11 n, 802.11g or 802.11 b standard.

    Note:

    Transmission standard IEEE 802.11n is still pending approval, which is likely to be granted in early 2008. Your Gigaset SE366 WLAN hardware is ready to comply with the new transmission standard. You might have to update the software for your device once standard compliant software is available (see page 84).

  Using a Gigaset SE366 WLAN makes it easy to set up a network at home or in small offices. For example, users can exchange data or share resources in the network, e.g. a file server or printer.

- **Security functions**

  The Gigaset SE366 WLAN offers comprehensive security measures:

  - Firewall protection against unauthorised access from the Internet

    All PCs in the local area network use the Public IP address of the Gigaset SE366 WLAN for their Internet connections, which makes them 'invisible' on the Internet. The Gigaset SE366 WLAN only allows access from the Internet if this has been requested from within the local area network.

    With the firewall, the Gigaset SE366 WLAN also offers comprehensive protection against hacker attacks.
  - Service filtering and URL filtering

    The Gigaset SE366 WLAN can filter Internet access. Here you determine which PCs may access which Internet services.

    In addition, you can deactivate access to certain Internet domains and sites (URL filtering).
  - Access control and encryption for the local wireless network

    You can use various encryption methods and authentication methods (WEP, WPA/WPA2-PSK,WPA/WPA2, MAC access control) to prevent unauthorised access to your wireless LAN or to make data illegible to unauthorised parties. The WPS feature allows you to establish a secure WLAN connection quickly and easily.
  - The sending power can be adjusted to suit local conditions. If you limit the reach of your wireless network to the size you need, you also make electronic eavesdropping more difficult.
- Other options
  - Exposed Host

    You can set up a PC on your local network to be a virtual server and release it for unrestricted access from the Internet.
  - Port forwarding

    You can release individual services on a PC that is integrated into the network.

Procedure for installation and configuration

1. First install an Ethernet network card or a wireless Network adapter such as the Gigaset PC Card 300 or the Gigaset USB Adapter 300 in the PCs you want to connect to the Gigaset SE366 WLAN. The installation process is described in the user guides for these products.

   Note:

   When installing wireless network adapters: The default SSID for the Gigaset SE366 WLAN is **ConnectionPoint**.

2. Make the necessary connections (PCs, modem) to the Gigaset SE366 WLAN and switch the device on (see the section entitled "Connecting the Gigaset SE366 WLAN" on page 22).
3. Before the PCs can communicate with the Gigaset SE366 WLAN and with each other in a local network, you must change their network settings. This will normally be the case if you are using the Windows default settings.

   To find out how to do this, read the document entitled “Network configuration” on the CD-ROM. First connect just **one** PC to the Gigaset SE366 WLAN. You can then carry out the basic configuration. After that you can connect further PCs.

   If your clients support WPS, you can establish the link from the PC's wireless network adapter to the Gigaset SE366 WLAN very simply: Push the registration button on the Gigaset SE366 WLAN and activate registration mode on the client. This is described on page 68 and in the user guide for the network adapter. You can also establish connections to other clients manually.
4. Configure the Gigaset SE366 WLAN to activate the device's Internet access (refer to the section entitled "Basic Setup Wizard" on page 31). To do this you will require access data from your Internet service provider.

If you want to use the Gigaset SE366 WLAN's other functions, e.g. the comprehensive security features, use the router's Security Setup (see page 35) or the ***Advanced Settings*** menu (see page 44).

First steps

Pack contents

The package contains the following items:

- One Gigaset SE366 WLAN,
- One mains adapter (100 V - 240 V / 12V DC 1A),
- One cable with RJ45 jacks (CAT5),
- One CD containing several documents (this user guide, description of the network configuration of PCs, license, warranty) and software for the language selection
- A Quick Start Guide.

System requirements

To operate your Gigaset SE366 WLAN you need:

- A PC with
  - an IEEE 802.11n (draft, see page 15), IEEE 802.11g or IEEE 802.11b compatible wireless Network adapter

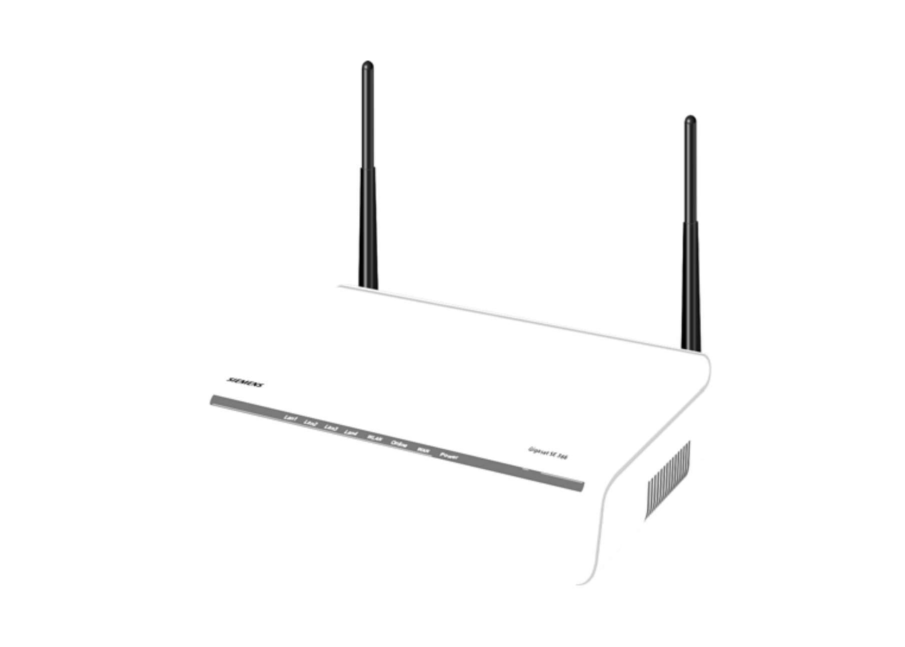
    Notes:
    The maximum theoretical data transfer rate for 802.11n-compatible network adapters is 300 Mbps, for 802.11g-compatible network adapters 54 Mbps, and for 802.11b-compatible network adapters 11 Mbps.

  or

  - an Ethernet connection
- A Web browser for configuration of your Gigaset SE366 WLAN (recommended products: Microsoft Internet Explorer 6.0 or higher and Mozilla Firefox 1.0 or higher)
- For Internet access
  - a DSL or cable modem and a splitter (for DSL)
  - the access data for your Internet Provider

Operating displays and connections

Front panel



LED displays

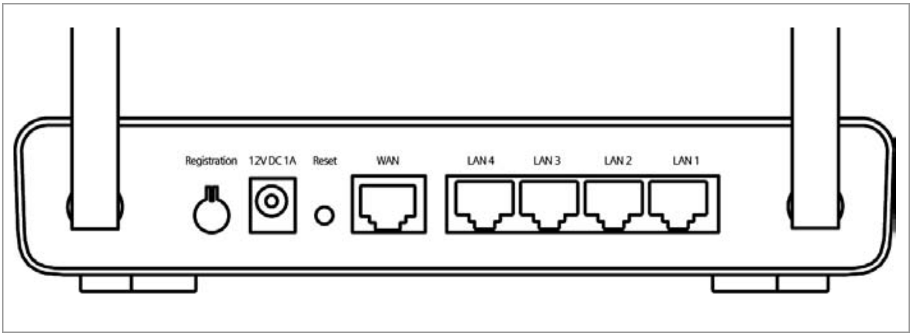
The front panel of the device contains LED displays that show the operating state and simplify installation and troubleshooting in the network.

The LEDs show the following (from right to left):

LED	State	Status
Power	On	The Gigaset SE366 WLAN is connected to the power supply.
	Off	The Gigaset SE366 WLAN is not connected to the power supply.
WAN	On	A DSL modem is connected to the WAN port.
	Flashing	The WAN port is sending or receiving data.
	Off	There is no modem connected.
Online	On	A connection to the Internet has been established (only for Internet connections via PPPoE and PPTP, see page 45)
	Off	There is no Internet connection.

LED	State	Status
WLAN	**In normal operation**	
	On	The radio interface is activated, no data transmission at present.
	Flashing	The Gigaset SE366 WLAN is sending or receiving data on the radio interface.
	Off	The radio interface is deactivated.
	During WPS registration	
	On (300 s)	WPS registration was successful.
	Flashing slowly	WPS registration is in progress.
	Flashing quickly	WPS registration was not successful.
	Flashing quickly with interruption	More than one client tried to register.
LAN1 – LAN4	On	A device is connected to the relevant LAN port.
	Flashing	The LAN port is sending or receiving data (traffic).
	Off	There is no device connected.

Back panel



The back panel of the Gigaset SE366 WLAN offers the following ports and controls:

Element	Description
Registration	Button for WPS activation. You can use this button to quickly establish a secure wireless connection to PCs. **Note:** You can deactivate the **Registration** button to protect it against unauthorised access (see page 86). The same function is provided via the device's user interface (see page 68).
12V DC 1A	Socket for the mains adapter that comes with the device. **Warning**: Using the wrong power supply unit may damage the Gigaset SE366 WLAN.

Element	Description
WAN	Socket for connecting to the DSL modem.
LAN4 – LAN1	Four 10/100 Mbps switch ports with automatic recognition (RJ45). You can connect up to four Ethernet devices (such as PCs, a Hub or Switch).

Reset

The reset button is located behind the small opening labelled **Reset**.

- Reboot function (software reset): Press the button for longer than 1 second but less than 5 seconds to reboot the device. This does not affect the configuration settings.
- Reset function (returns to factory settings): Press and hold the button for at least 5 seconds to return all settings to the factory settings.
  Warning: This will clear all the configuration settings you have made since the initial startup. This also applies for the data generated with WPS for the wireless network (SSID and pre-shared key).

Setting up the Gigaset SE366 WLAN

The Gigaset SE366 WLAN can be set up in any suitable location in your home or office. You do not need any special wiring. However you should comply with the following guidelines:

- Place the device away from heat sources, direct sunlight and other electrical devices.
- Do not place the device on a heat-sensitive surface.
- Do not place objects on the device. Ensure that all air openings for air circulation are not blocked.
- Lay the cables so that nobody can trip over them.
- Position the device on a non-slip surface.
- A suitable socket as well as a connection to the Ethernet interface of a PC or a wired network must be available in the place where you set up the Gigaset SE366 WLAN.
- Do not position the device in the immediate vicinity of stereo equipment, TV sets or microwave ovens. This may cause interference.
- For wall mounting: Make sure not to damage any pipes or cables in the wall when drilling the dowel holes.

Instructions for use

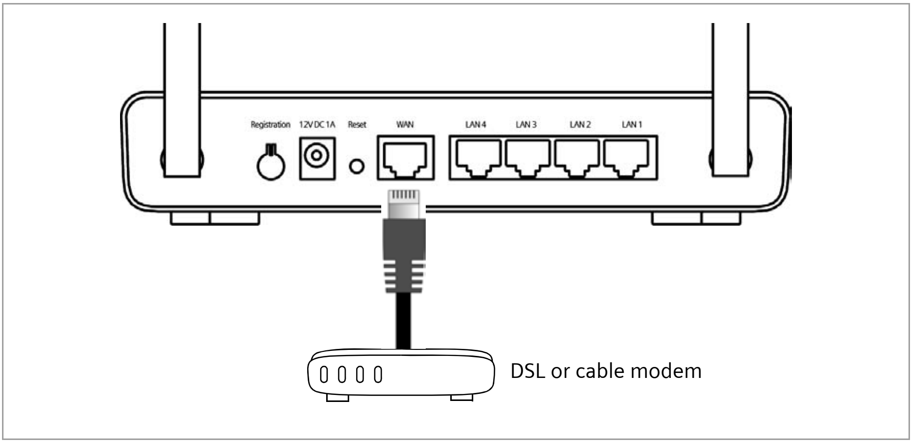
- Never open or repair the device or mains adapter. For reasons of electrical safety it may only be opened by authorised service technicians.
- Never touch the pin and socket contacts with sharp or metallic objects.
- Do not touch the mains adapters with wet hands.
- Use an antistatic cloth to clean the device. Cleaning agents or solvents are not suitable.

Connecting the Gigaset SE366 WLAN

Before starting to connect PCs to your Gigaset SE366 WLAN, make sure that a wired or wireless Network adapter is connected to the PC. Please read the user guide that came with the device. Newer PCs and notebooks have wired Ethernet adapters, and often wireless adapters, built in at the factory.

Connecting to the DSL or cable modem

→ Connect the socket on the back of the router marked **WAN** to your DSL or cable modem with an Ethernet cable.



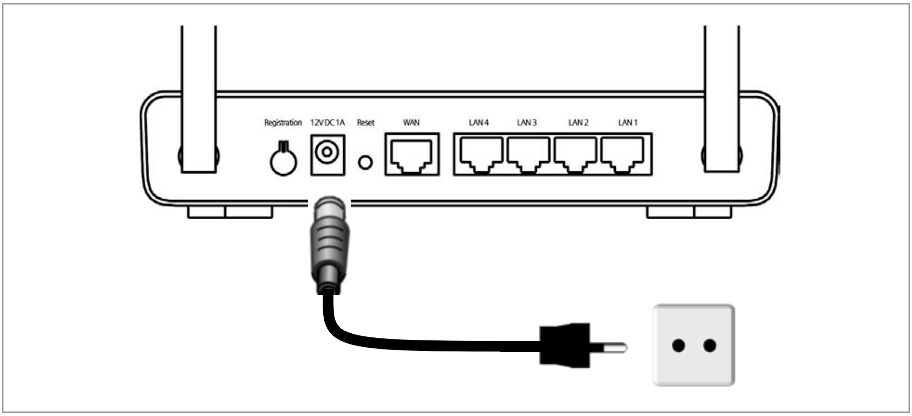
Note:
Use a category 5 Ethernet cable with RJ45 jacks on both ends for all connections. The cable will normally be included with your modem. However, you can also use the yellow Ethernet cable, which comes with the Gigaset SE366 WLAN.

Connecting to the mains power supply

Note:
Only use the mains adapter (12V DC 1A) that is supplied with the device.

→ Connect the mains adapter cable to the **12 V DC 1A** socket on the Gigaset SE366 WLAN.

→ Plug the mains adapter into a mains socket.



Connecting PCs wirelessly via WPS

If you are using WPS (see page 13), you can connect wirelessly to other WLAN devices quite simply via the registration button.

→ Press the registration button for at least two seconds on the device’s back panel to start WPS registration.

→ Within two minutes, activate WPS registration of the wireless network adapter on the PC. The client gets the security data for the Gigaset SE366 WLAN (SSID and pre-shared key) and is thereby registered.

WLAN LED display during WPS registration:

On (300 s)	WPS registration was successful.
Flashing slowly	WPS registration is in progress.
Flashing quickly	WPS registration was not successful.
Flashing quickly with interruption	More than one client tried to register.

Only one client is allowed to register during a single registration phase. If the device indicates by means of the WLAN LED that more than one client has tried to register, and the desired client has not been registered successfully, an external device may have connected to your WLAN. In this case, you should change the WPA-PSK key as quickly as possible (see page 39) and perform the WPS registration for the clients using a PIN (see page 68).

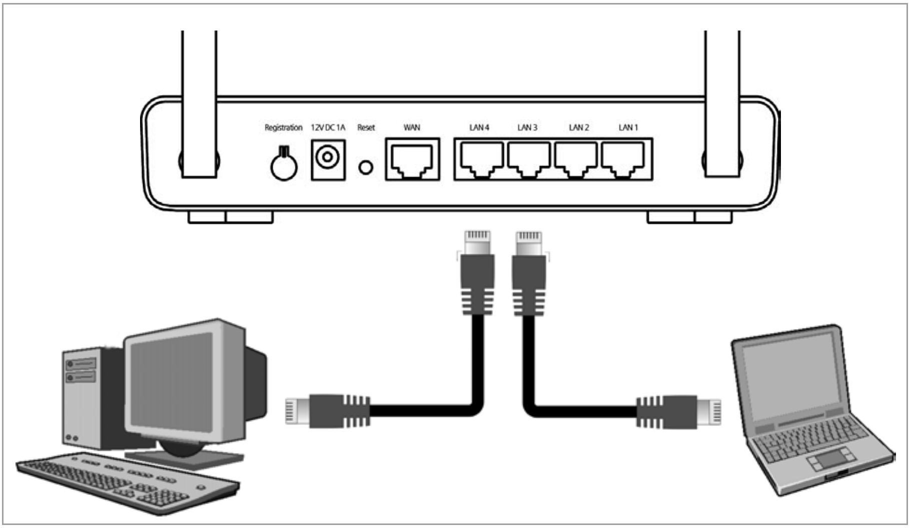
Additional options for WPS registration are described on page 68.

Connecting PCs in wired mode

If you are not using WPS, we recommend that you first connect the device to a PC using an Ethernet cable. Depending on use, you will first have to make some settings via the browser-based configuration program of your Gigaset SE366 WLAN.

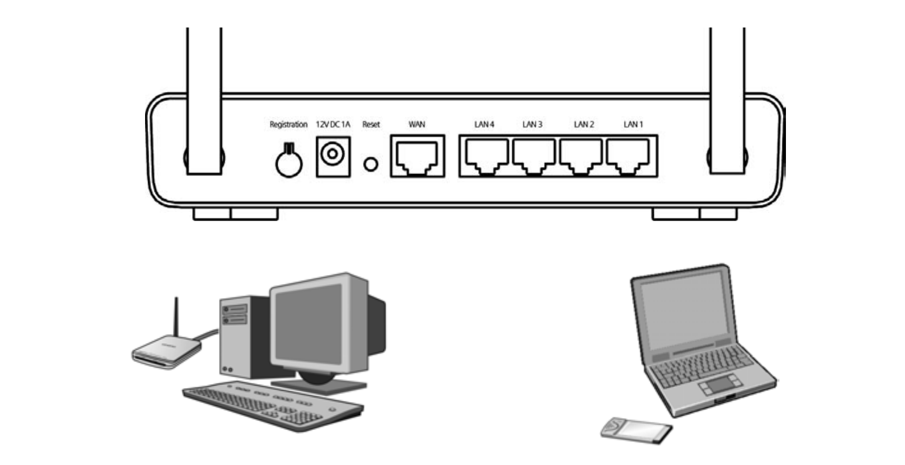
→ Connect one of the yellow LAN sockets (**LAN1** – **LAN4**) at the rear of the Gigaset SE366 WLAN to the Ethernet connection on a PC. To do this, use an Ethernet cable with RJ45 jacks. You can also use the yellow Ethernet cable supplied with the device.

The four LAN connections can automatically set the transmission speed to 10 Mbps Ethernet or 100 Mbps Fast Ethernet, and the transmission mode to Half duplex or Full duplex depending on the performance of the network adapter in your PC.



Connecting wirelessly to a PC without WPS

A wireless connection is made using a wireless network adapter that must be installed in your PC. For example, this can be a Gigaset PC Card 300 or another 802.11n, 802.11g or 802.11b-compatible wireless network adapter.



You define a Radio network by assigning all the devices an identical SSID and setting the same encryption.

Assign the SSID of the Gigaset SE366 WLAN to the network adapters. The factory set SSID is **ConnectionPoint**. If the correct SSID has been entered in your PC's wireless network adapter, the wireless link will be established automatically once you connect your Gigaset SE366 WLAN to the mains power supply (see page 25). You should then configure encryption on the Gigaset SE366 WLAN and the wireless network adapter.

Your Gigaset SE366 WLAN is now ready for use:

- The **power** LED on the front lights up.
- The **WLAN** LED lights up to indicate that the Gigaset SE366 WLAN is ready to open wireless connections.

  The radio link to a PC that is connected by means of a wireless network adapter is established automatically if the network adapter has been configured with the same SSID as the Gigaset SE366 WLAN (see page 25). It can take a few seconds for the wireless connection to be established. The **WLAN** LED flashes when data is sent or received via this connection.
- The **LAN** LEDs light up if a device is connected to the respective LAN port by means of an Ethernet cable.

In order to communicate via the Gigaset SE366 WLAN, the network must be configured on the connected PCs. This usually happens automatically. To find out more about this, refer to the document “Configuring the local network” on the CD.

The user interface

Once you have configured the network settings on a PC in your local network, you can then use that PC to configure the Gigaset SE366 WLAN with the aid of the Gigaset SE366 WLAN's user interface. You can use any browser for the configuration; the recommended products are Microsoft Internet Explorer 6.0 or higher and Mozilla Firefox 1.0 or higher.

Note:

To start the configuration environment, you might need to deactivate the HTTP proxy for your browser (see page 93).

If you use Mozilla Firefox or if you use Internet Explorer and Windows XP Service Pack 2, you need to configure the popup blocker (see page 93).

Launching the user interface

To access the Gigaset SE366 WLAN's user interface:

→ Launch your Web browser.

→ Enter the IP address of the Gigaset SE366 WLAN in the browser's address field.

```
http://192.168.2.1
```

When the configuration program is opened for the first time or if the device has been switched back to the factory settings, the default settings assistant is started (see page 31).

Otherwise the registration page for entering the password will appear.

→ Enter the password and click ***OK***.

The default password on delivery is ***admin***.

Note:

For security reasons you should change the password at a later stage (see page 35).

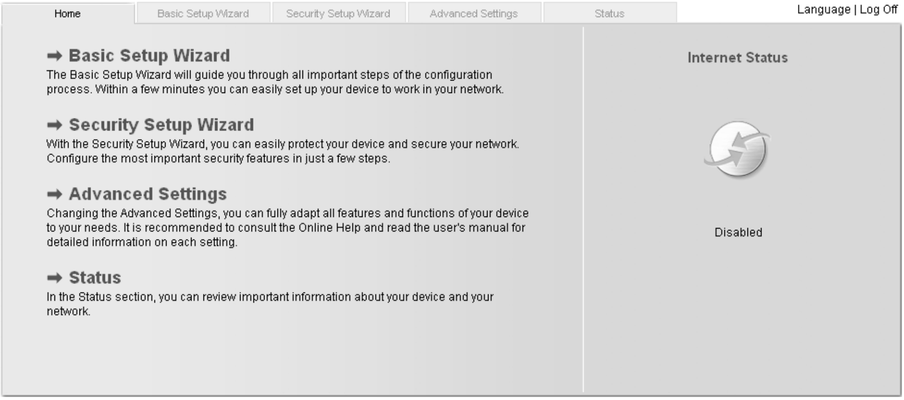
A page containing security information is displayed.

→ Click ***OK***.

You will now see the start screen.

The start screen

The start screen is the starting point for all configuration and administration activities.



➡ **Basic Setup Wizard**

The Basic Setup Wizard will guide you through all important steps of the configuration process. Within a few minutes you can easily set up your device to work in your network.

➡ **Security Setup Wizard**

With the Security Setup Wizard, you can easily protect your device and secure your network. Configure the most important security features in just a few steps.

➡ **Advanced Settings**

Changing the Advanced Settings, you can fully adapt all features and functions of your device to your needs. It is recommended to consult the Online Help and read the user's manual for detailed information on each setting.

➡ **Status**

In the Status section, you can review important information about your device and your network.

Internet Status

Disabled

Start screen functions

On the start screen you can

- select the language for the user interface (see page 29),
- connect to the Internet (see page 77),
- call up the basic setup wizard, see Basic Setup Wizard (see page 31),
- call up the wizard for Security Setup Wizard (see page 35)
- open the ***Advanced Settings*** menu for additional configuration options (see page 44),
- open the ***Status*** menu to obtain status information about the Gigaset SE366 WLAN (see page 77),

You can call up the wizards, the ***Advanced Settings*** menu and status information from any other screen in the configuration program at any time via the tabs at the top edge of the user interface.

The configuration program offers you the following functions:

Basic Setup Wizard
Use this wizard to make the settings required for connecting to the Internet. You can also set the data for your region. This is described on and after page 31.

Security Setup Wizard
This wizard allows you to take precautions against unauthorised access to your Gigaset SE366 WLAN and the local network. For example, you can assign a password and set up encryption for wireless traffic. This is described on and after page 35. For the protection of your network we recommend that you execute this wizard.

Advanced Settings
Additional functions are offered in the ***Advanced Settings*** menu. For example, you can back up and restore your configuration data, define access control for PCs, and much more. These configuration steps are optional and can be carried out at a later stage. This is described on and after page 44.

Status
You can view information about the configuration and status of your Gigaset SE366 WLAN in the ***Status*** menu. This is described on and after page 87.

Internet Status
You can view the status of your Internet connection and establish a manual connection to the Internet (see page 77).

Language
You can select the language for the user interface (see page 29).

Selecting a language

The user interface can be presented in various languages. During the initial configuration or after resetting the device to the factory settings, the user interface is displayed in German (if the Web browser is also in German) or in English (for all other languages).

- Click ***Language*** at the top right above the Start screen.
- If you wish to change the preset language, select the required language from the list.
- Click ***OK*** to apply the setting.

You might have to load the file for the language you require. The files are either on the CD-ROM or you can download other languages from the Internet and save them on your PC. Follow the on-screen instructions on the user interface page.

Reboot the device to activate the change. Confirm the reboot in the dialogue field on the screen.

Once the procedure is complete the start screen is shown again.

Elements on the user interface

The user interface Web pages contain the following elements:

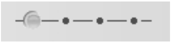
Log Off button

You will always find the ***Log Off*** button on the right above the user interface. If you click ***Log Off***, the session is terminated and the login screen appears again.

Help

Click the question mark to display explanations about the current user interface screen.

Buttons and symbols used by the wizards



The wizards use graphic symbols to show which steps you have already carried out.

As soon as you have changed the configuration in a screen, you can activate the new setting by clicking ***Next >*** at the bottom of the screen. The ***< Back*** button returns you to the previous configuration step and ***Cancel*** returns you to the start screen.

Buttons in the *Advanced Settings* menu

OK Transfers the settings you have made to the Gigaset SE366 WLAN configuration.

Cancel Deletes all the entries on a screen since the last time you clicked ***OK***. This button is not available for the initial configuration of the device.

Other buttons may be visible depending on the function in question. These are described in the relevant sections.

Basic Setup Wizard

The Basic Setup Wizard guides you step by step through the general configuration of the Gigaset SE366 WLAN. This includes settings for your region and for your Internet access.

Connection to the Internet is established via the Gigaset SE366 WLAN for all PCs connected to it. You will need your Internet Provider's access data for configuration. You should therefore have this data to hand.

Note:

The Basic Setup Wizard will reconfigure your Internet settings if you have already set them. This does not affect the WLAN and LAN settings.

The access data is stored in the Gigaset SE366 WLAN during configuration. Before passing the device on to somebody else or having your dealer replace it, you should first restore the configuration to the factory settings (see page 83). If you do not, unauthorised persons will be able to use your Internet access data at your expense.

During initial configuration, the start screen of the ***Basic Setup Wizard*** is displayed automatically.

→ If you want to execute the Basic Setup Wizard again after the initial configuration, select the ***Basic Setup Wizard*** entry on the start screen to start configuration.

→ Click ***Next >***.

Regional Options

On this screen you select your present location for the regional settings.

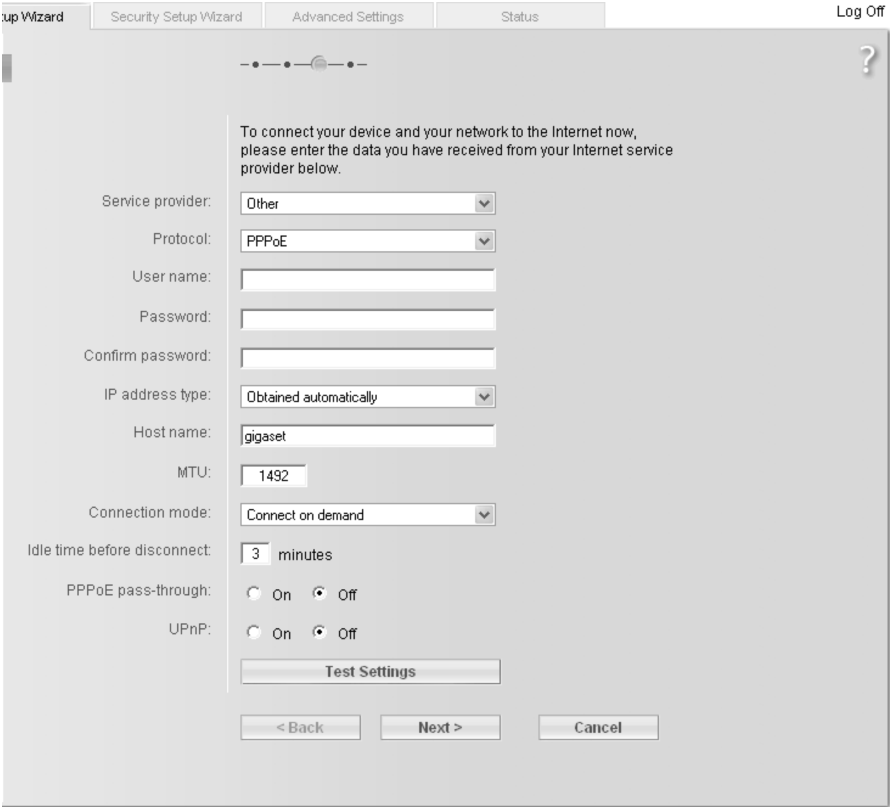
→ Select the country in which you are currently located from the list. You can decide to have the clock change automatically to summer time and/or to the time zone as you wish.

→ Select the required option and/or select the time zone for your location.

→ Click ***Next >***.

Configuring Internet connections

You will find the access data you need for configuring the Internet connection in the documentation you receive from your Internet Provider (ISP).



To connect your device and your network to the Internet now, please enter the data you have received from your Internet service provider below.

Service provider: Other

Protocol: PPPoE

User name:

Password:

Confirm password:

IP address type: Obtained automatically

Host name: gigaset

MTU: 1492

Connection mode: Connect on demand

Idle time before disconnect: 3 minutes

PPPoE pass-through: ○ On ● Off

UPnP: ○ On ● Off

→ Select your service provider from the ***Service provider*** selection menu. If your Internet provider is not included in the list, select ***Other***.

The list of Internet service providers offered depends on your choice of country in the ***Regional Options***.

→ Enter the data you have been given by your Internet provider.

When you choose your Internet provider from the list, most of the data you need is entered by default on the screen.

You can also often confirm the defaults for the ***Other*** option.

Check that the Protocol complies with the data supplied by your Internet provider.

> **Note:**
>
> Connection to the Internet is only possible if you have entered all the data of your Internet provider correctly.

→ Select how Internet sessions are to be established via the ***Connection mode***:

- Select ***Always on*** if the connection is to remain set up when the Gigaset SE366 WLAN is switched on.

  > **Note:**
  >
  > If you subscribe to a time-based service, this option can result in high connection charges.

- Select ***Connect on demand*** if applications such as a Web browser or an e-mail program are allowed to connect to the Internet automatically.
- In the ***Idle time before disconnect*** field, enter a period of time after which the Internet connection is to close down automatically if no data is transmitted (default setting: 3 minutes, range: 1 to 99 minutes).

  This time setting only applies to the ***Connect on request*** option. A permanent connection is achieved using the ***Always on*** option.
- Select ***Connect manually*** if you always want to establish and end the connection to the Internet manually. If you subscribe to a time-based service this will save you high connection charges. How to establish a connection manually is described on page 82.

→ Click ***Test Settings*** to check the Internet connection. The device will attempt to connect to the Internet. Any existing Internet connection will be closed first.

You will find information about the test steps and results on the ***Internet Connection Test*** screen.

PPPoE pass-through

PPPoE pass-through enables you to use an additional Internet connection (with another service provider) from one PC. You can find detailed information about this on page 47.

→ Activate ***PPPoE pass-through*** if you wish to use this function.

Using UPnP (Universal Plug & Play)

PCs with UPnP (Universal Plug & Play) can offer their own network services and automatically use services offered on the network. You can find detailed information about this on page 48.

→ Activate ***UPnP*** if you wish to use this function.

→ Click ***Next >***.

Summary

In the next step the basic settings you have made with the wizard are shown for you to check.

→ If you want to make changes to the settings, click
< Back.

→ If you want to confirm the settings, click ***Finish*** to close the Basic Setup Wizard.

You will then be taken automatically to the start screen for the ***Security Setup Wizard***. If you want to carry this out at a later stage, deactivate the option ***I would like to run the Security Setup Wizard now.***

The Gigaset SE366 WLAN is now configured and ready to connect to the Internet.

Security settings

The ***Security Setup Wizard*** offers you additional settings that will improve your network security. You can

- assign a password for configuring the Gigaset SE366 WLAN (see page 35),
- change the ID for your wireless network (SSID) (see page 37),
- set Encryption for wireless traffic (see page 38),
- limit access to your wireless network to certain PCs (see page 42).

The Gigaset SE366 WLAN's user interface will guide you through the security configuration step by step. Once you have completed a screen, click ***Next >***. If you want to make any changes or check your entries, click ***< Back***.

→ Select ***Security Setup Wizard*** on the start screen or on the tab to start the security configuration if you did not go straight to the start screen for the security settings after making the basic settings.

→ Click ***Next >*** to proceed to the next step.

When using WPS please note the following:

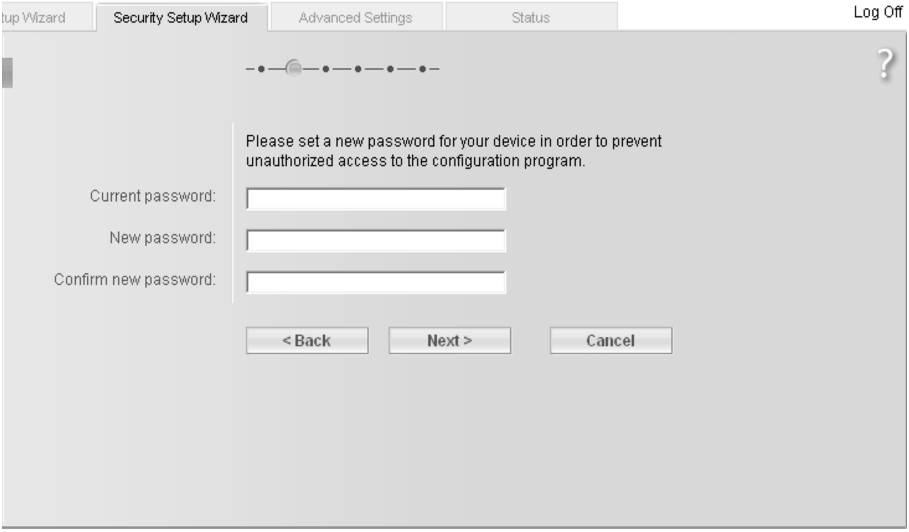
Your Gigaset SE366 WLAN is equipped with WPS (Wi-Fi Protected Setup). You can use it to set the security of your wireless network easily with one click only (see page 13).

An SSID and a pre-shared key are created automatically by pressing the **Registration** button on the device’s back panel (see page 20), thus allowing synchronisation of the WPS-enabled clients.

You can inspect the defined settings in the ***Security Setup Wizard*** (see page 37 and page 39) or in the Advanced Settings (see page 70).

Changing the password

In the first step of the assistant the password for the user interface can be changed. On delivery, the configuration of your Gigaset SE366 WLAN is protected with the ***admin*** password. To prevent unauthorised changes to the configuration, you should set your own password and change this password from time to time.



Please set a new password for your device in order to prevent unauthorized access to the configuration program.

Current password:

New password:

Confirm new password:

→ Enter the default password (or the new password you have assigned) in the ***Current password*** field.

→ Enter a new password in the ***New password*** field and repeat it in the ***Confirm new password*** field.

The password can be up to 32 alphanumeric characters long. The password is case sensitive. Avoid proper names and all too obvious words. Use a combination of letters and numbers.

Note:

If you ever forget your password you will have to return the Gigaset SE366 WLAN to its factory settings (see page 20). ***admin*** is then again assigned as the password. Please bear in mind that this will return all the configuration settings to the factory settings.

→ Click ***Next >*** to proceed to the next step.

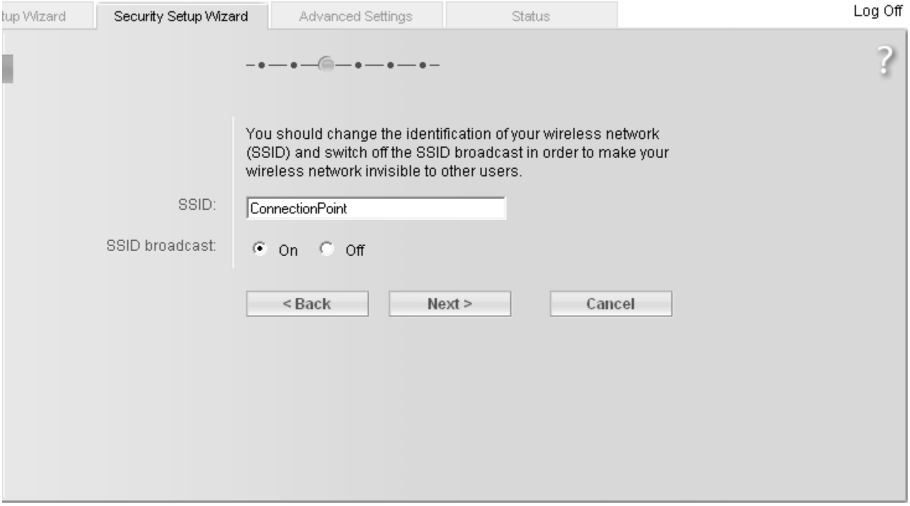
SSID

Before the wireless network components can communicate with each other, they must all use the same SSID (Service Set Identifier).

On delivery, the Gigaset SE366 WLAN's default SSID is **ConnectionPoint**.

Note:

- If you already have performed WPS registration (see page 68), you will see the generated SSID on this screen. Do not change the SSID in this case. Otherwise, you will have to register all connected clients again. You may even have to perform a factory reset of your Gigaset SE366 WLAN.
- If you are not using WPS, you should change the SSID for security reasons. You have to make this change on all wireless network adapters.



You should change the identification of your wireless network (SSID) and switch off the SSID broadcast in order to make your wireless network invisible to other users.

SSID: ConnectionPoint

SSID broadcast: ● On ○ Off

→ Enter a character string of your choice in the ***SSID*** field. The SSID is case sensitive. It can be up to 32 alphanumeric characters long.

Make a note of the SSID. You will need it to configure your wireless network adapter.

Note:

The connection to the wireless network adapters will be interrupted until the new SSID has been entered in them as well.

SSID broadcast

If this option is enabled (default), the Gigaset SE366 WLAN will send the SSID in all data transmissions and your Gigaset SE366 WLAN's SSID will be displayed on all PCs that have a wireless network adapter. In this case, eavesdroppers could use the SSID to gain access to your local network.

→ Select ***Off*** to deactivate ***SSID broadcast.***

→ Click ***Next >*** to proceed to the next step.

Setting security functions for the wireless network

In the next step you can set the encryption and authentication methods for your wireless network.

Wireless networks are even more strongly exposed to the risk of eavesdropping than wired networks. With conventional network adapters an intruder only needs a device with a WLAN adapter (e.g. a notebook or a PDA (Personal Digital Assistant)) with an appropriately configured network card in order to eavesdrop on every communication made via a nearby wireless LAN.

The Gigaset SE366 WLAN uses effective encryption methods to largely prevent eavesdropping.

You can use the following security mechanisms:

◆ WPA2-PSK or WPA2-PSK / WPA-PSK (see below)

◆ WEP encryption (Wired Equivalent Privacy, see page 40)

We recommend using WPA2-PSK if it is supported by all components in your wireless network.

WEP encryption is not supported if you are using WPS.

You will find further options for setting data encryption and authentication in the ***Advanced Settings*** menu (see page 69).

WPA2 / WPA with pre-shared key (PSK)

WPA is a more advanced procedure than WEP for protecting wireless networks. Dynamic keys based on TKIP (Temporal Key Integration Protocol) offer increased security. The new WPA2 standard uses AES for encryption.

WPA-PSK is a special WPA mode for users at home and in small companies without a company authentication server. Encryption keys are automatically generated with the pre-shared key, automatically changed ("rekeying") and authenticated between the devices after a certain period of time (Rekey interval).

Every PC (network adapter) that requires access to a wireless network protected by WPA must also support WPA. To find out whether and how you can use WPA on your PC, refer to the user guide supplied with your network adapter.

If a PC is already successfully registered via WPS, this screen shows the generated pre-shared key. The pre-shared key in the advanced settings can be viewed in plain text on the ***Wireless Network*** – ***Encryption*** page.

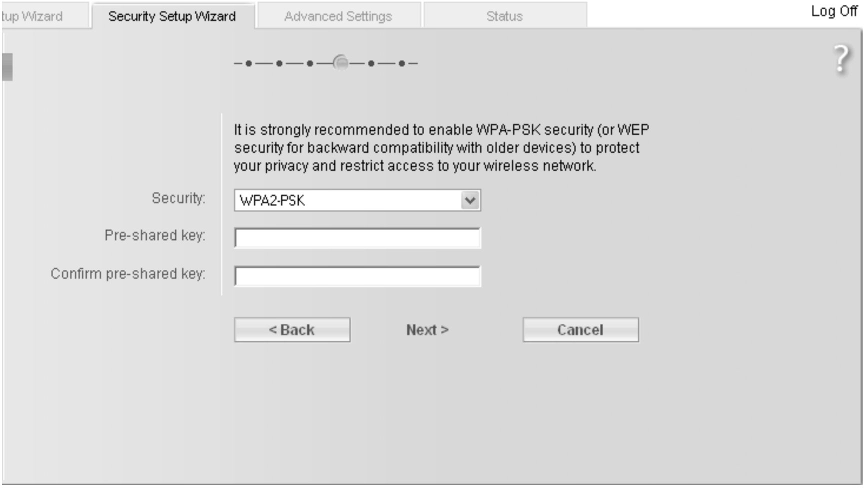
→ Click ***Next >*** to reach the next step.

If you are not using WPS:

→ Select the ***WPA2-PSK*** option if it is supported by all components in your wireless network.

or

→ Select ***WPA2-PSK / WPA-PSK*** if some or all components in your wireless network support WPA with the TKIP protocol.



It is strongly recommended to enable WPA-PSK security (or WEP security for backward compatibility with older devices) to protect your privacy and restrict access to your wireless network.

Security: WPA2-PSK

Pre-shared key:

Confirm pre-shared key:

→ Enter a key of your choice in the ***Pre-shared key*** field (min. 8 to max. 63 characters) and confirm it by repeating the entry.

Note:

- ◆ It is very **important** that you make a note of the ***Pre-shared key***. You will need this information to configure the wireless network adapters correctly.
- ◆ When you have completed the Security Setup Wizard you must also change the encryption data of the wireless network adapters in the connected PCs since, without the change, they will not be able to access the Gigaset SE366 WLAN's wireless network.

→ To go to the next step, click ***Next >***.

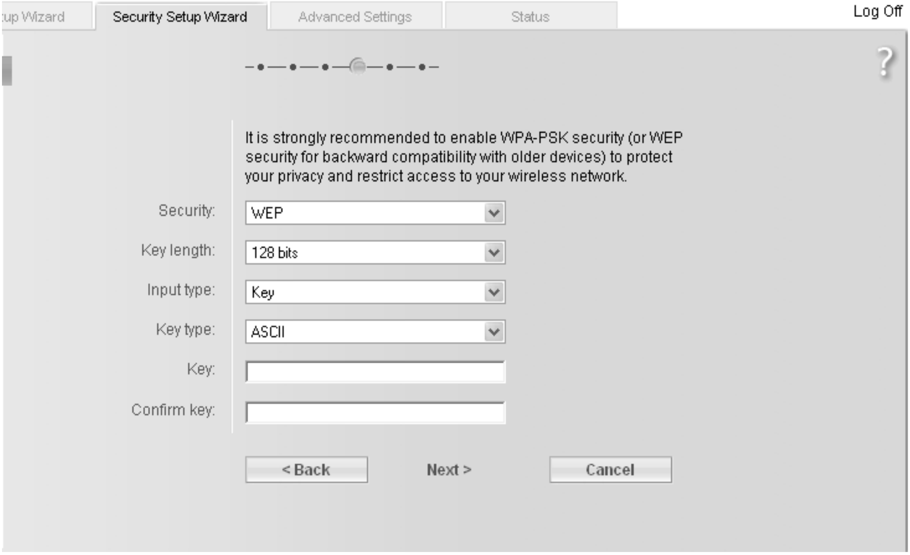
WEP encryption

WEP (Wired Equivalent Privacy) is an encryption procedure for radio signals in wireless networks and complies with the IEEE 802.11 standard.

If you transmit data wirelessly and not all components in your wireless network support the higher security standard WPA (see page 39), we recommend that you activate WEP Encryption on these network components.

You cannot user WEP together with registration via WPS.

You can choose either the standard 64-bit keys or the more robust 128-bit keys for encryption. The keys are generated in hexadecimal or ASCII format. You must use the same keys for the Gigaset SE366 WLAN and all your wireless network adapters.



It is strongly recommended to enable WPA-PSK security (or WEP security for backward compatibility with older devices) to protect your privacy and restrict access to your wireless network.

Security:	WEP
Key length:	128 bits
Input type:	Key
Key type:	ASCII
Key:	
Confirm key:	

→ Select the ***Key length***: 64 or 128-bit.

→ Select the ***Input type***, i.e. whether you wish to enter the key manually or have it generated automatically by means of a ***Passphrase***.

Manual key entry

→ Select the ***Key type***, ***Hex*** or ***ASCII***.

If you select ***Hex*** as the key type, you can use the characters **0** to **9** and **A** to **F**.

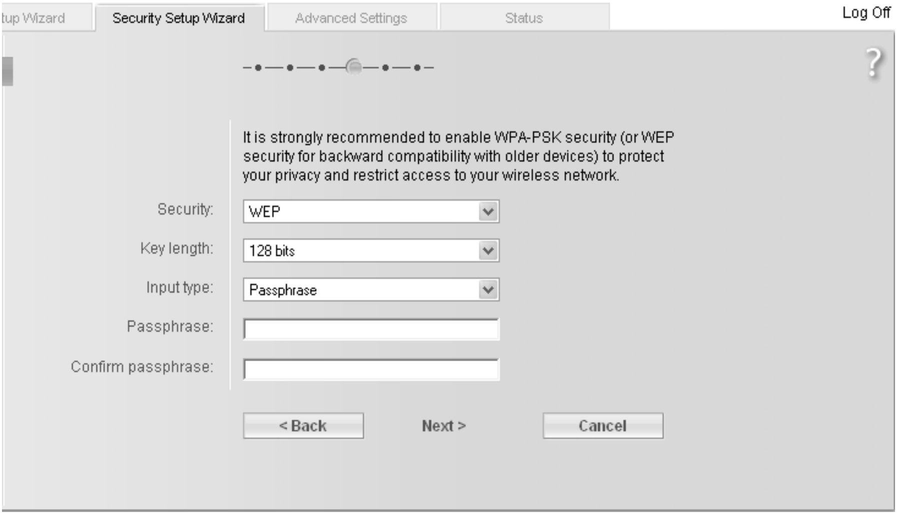
- With a 64-bit encryption depth the key is exactly 10 characters long (Example of a valid key: 1234567ABC)
- With a 128-bit encryption depth the key is exactly 26 characters long (Example of a valid key: 234567ABC8912345DEF1234567)

If you select ***ASCII*** as the key type, you can use the characters **0** to **9**, **A** to **Z**, and **a** to **z** plus the special characters in the ASCII character set.

- With a 64-bit encryption depth the key is exactly 5 characters long. (Example of a valid key: GIGA1)
- With a 128-bit encryption depth the key is exactly 13 characters long. (Example of a valid key: GIGASET_SE336)

→ Confirm the key by entering it again in the field ***Confirm key***.

Generating the key by means of a Passphrase



It is strongly recommended to enable WPA-PSK security (or WEP security for backward compatibility with older devices) to protect your privacy and restrict access to your wireless network.

Security: WEP

Key length: 128 bits

Input type: Passphrase

Passphrase:

Confirm passphrase:

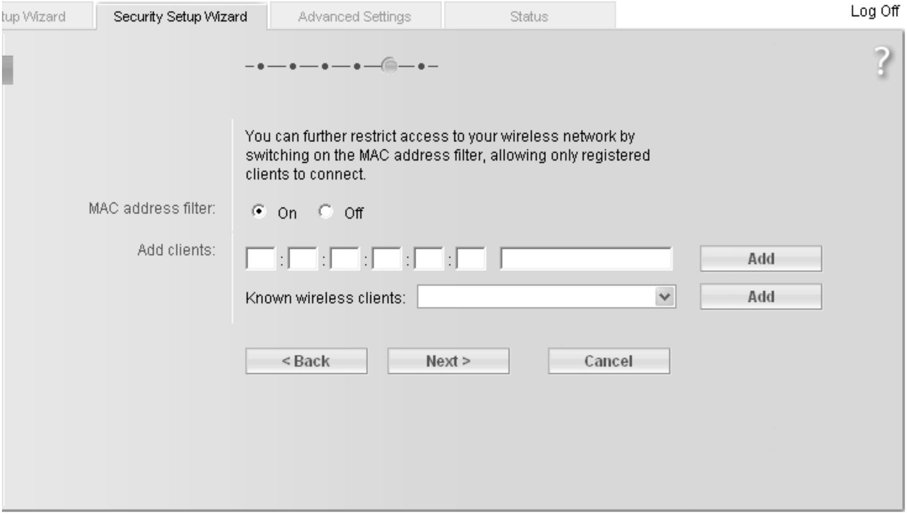
→ Enter a ***Passphrase*** (up to 32 characters) and confirm it by entering it again. The key is generated automatically.

Note:
- It is very **important** that you make a note of the key or passphrase. You will need this information to configure the wireless network adapters correctly.
- When you have concluded the Security Setup Wizard you must also change the WEP encryption data of the wireless network adapters in the connected PCs since, without the change, they will not be able to access the Gigaset SE366 WLAN's wireless network.

→ To go to the next step in the Security Setup Wizard, click ***Next >***.

Access control within the wireless network

In this step you can specify which PCs will have wireless access to the Gigaset SE366 WLAN and hence to your LAN. Access control is based on the MAC addresss of the PCs' network adapters. You can enter the MAC addresses for the PCs manually or select them from the list of PCs that are currently logged in.



You can further restrict access to your wireless network by switching on the MAC address filter, allowing only registered clients to connect.

MAC address filter: ● On ○ Off

Add clients: [ ]:[ ]:[ ]:[ ]:[ ]:[ ] [ ] Add

Known wireless clients: [ ] Add

< Back | Next > | Cancel

The default setting for access control is disabled. This means that all PCs that use the correct SSID and the right encryption method can log in.

→ Next to ***MAC address filter*** select the option ***On*** to activate MAC filtering.

Entering MAC addresses manually

→ Enter the MAC address of the network adapter. You will normally find this address on a label on the device.

→ Enter a name for the PC.

→ Click ***Add*** to add the entry to the list.

Selecting from the list of known PCs

→ Select the required PC from the ***Known wireless clients*** list. All PCs that are currently logged in to the router with the correct SSID are displayed.

→ Click ***Add*** to add the selected PC to the list.

Note:

- If you have activated MAC access control and want to use WPS, please note that only clients already included in the MAC address list can register via WPS.
- If you activate MAC access control, you must at least enter the PC from which you are configuring the Gigaset SE366 WLAN. If you fail to do this, you will no longer be able to access the user interface and an error message will be shown.
- If, by mistake, you have denied all PCs access to the Gigaset SE366 WLAN you have two options:
  - You can reset the Gigaset SE366 WLAN to the factory settings (see page 20).
  - You can connect a PC to the Gigaset SE366 WLAN using one of the LAN connections (by cable). Since MAC access control only applies to PCs that are connected "wirelessly", you can use this PC to change the configuration.

→ To go to the next step, click ***Next >***.

Saving settings

On the next screen you close the wizard and save the settings. You will be informed of any security risks that still exist.

→ Click ***Finish*** to close the wizard.

The settings will now be active on your Gigaset SE366 WLAN.

Note:

You must now configure the WEP or WPA key for your PC's wireless network adapter, if this has been configured with other values. Once you have done this you can log in to your Gigaset SE366 WLAN wirelessly again.

Configuring the Advanced Settings

You can configure all the options for the Gigaset SE366 WLAN in the ***Advanced Settings*** menu. If you want, you can also make changes to the settings you made using the wizard. The following table shows the options in the menu.

range

Menu	Description
Internet	This menu comprises all the settings relating to the Internet. You can: ◆ check and change the configuration for Internet access (see page 45) or specify a preferred DNS server (see page 49), ◆ configure the firewall, i.e. a number of security and special functions, e.g. access control for local PCs to the Internet or blocking certain Internet sites (see page 50), ◆ make the NAT settings needed to provide your own services on the Internet (see page 56), ◆ set up dynamic DNS for a static Internet address on your device (see page 61), ◆ configure the Quality of Service (see page 62).
Local Network	You can change the Private IP address of the Gigaset SE366 WLAN here and make settings on the DHCP server (see page 63).
Wireless Network	You can define your settings for WPS here, configure the options for wireless communication (SSID and encryption) and restrict access to the Gigaset SE366 WLAN (see page 45). In addition, you can optimise the transmission quality of your WLAN and adjust it to your requirements (range, transmission rate, see page 65).
Administration	You can make or change various system settings here, e.g. assign a password (see page 79), set the time (see page 78), or activate remote administration (see page 80). You can also back up the data on your Gigaset SE366 WLAN or load new firmware (see page 82).

Configuring the Internet connection

If you have configured your Gigaset SE366 WLAN using the two wizards, you will already have configured the WAN connection (Internet access). You can check or change these settings in the ***Internet*** menu.

This menu also offers you a wide range of options for security settings and for limiting access to the Internet as well as for providing your own services on the Internet.

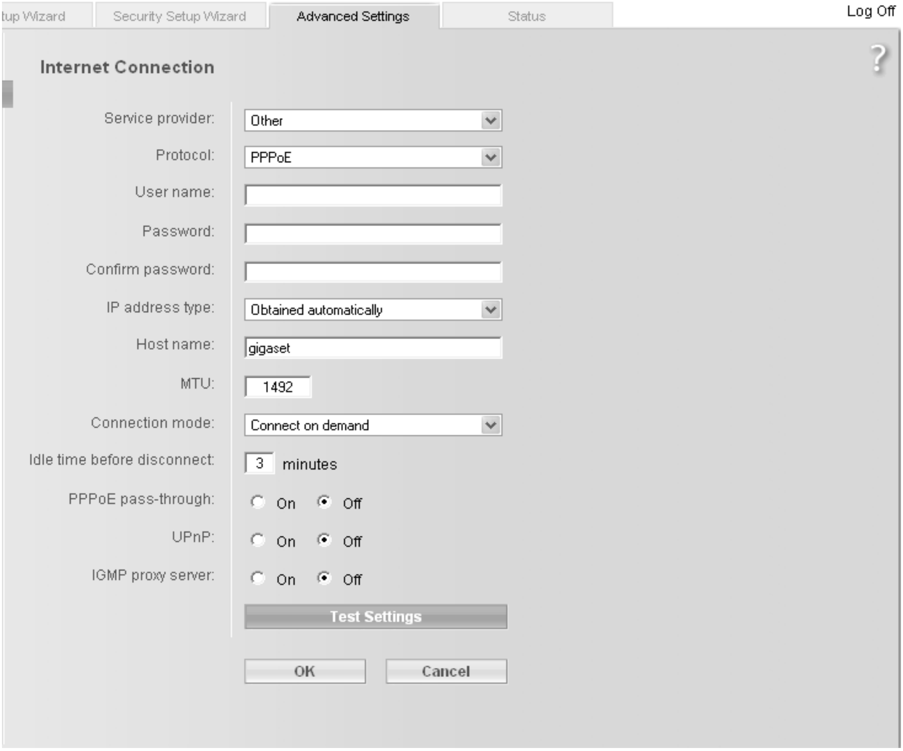
Internet

On the ***Internet*** screen you can grant or block access to the Internet over your Gigaset SE366 WLAN.

Internet Connection

You can set up or change the configuration of your Internet connection on this screen. Any settings you make here must coincide with the features your Internet provider makes available to you. Incorrect data can lead to problems with your Internet connection.

→ If you wish to set up or change the settings for the Internet connection, select ***Internet Connection*** in the ***Advanced Settings*** – ***Internet*** menu.



Internet Connection

Service provider:	Other
Protocol:	PPPoE
User name:	
Password:	
Confirm password:	
IP address type:	Obtained automatically
Host name:	gigaset
MTU:	1492
Connection mode:	Connect on demand
Idle time before disconnect:	3 minutes
PPPoE pass-through:	○ On ● Off
UPnP:	○ On ● Off
IGMP proxy server:	○ On ● Off

→ Select your Internet provider from the ***Service provider*** list.

The list of Internet providers offered depends on your choice of country under ***Regional Options***.

→ Enter the data you have been given by your ***Service provider*** in the relevant fields.

When you choose your Internet provider from the list, most of the data you need is entered by default on the screen.

You can also often confirm the defaults for the ***Other*** option.

Check that the Protocol complies with the data supplied by your Internet provider.

Note:
To configure the Internet connection successfully all fields must be filled in with the precise details given by your provider.

→ Select how Internet sessions are to be established via the ***Connection mode***:

- Select ***Always on*** if the connection is to remain set up when the Gigaset SE366 WLAN is switched on.

  Note:

  If you subscribe to a time-based service, this option can result in high connection charges.

- Select ***Connect on demand*** if applications such as a Web browser or an e-mail program are allowed to connect to the Internet automatically.
- In the ***Idle time before disconnect*** field, enter a period of time after which the Internet connection is to close down automatically if no data is transmitted (default setting: 3 minutes, range: 1 to 99 minutes).

  This time setting only applies to the ***Connect on demand*** option. A permanent connection is achieved using the ***Always on*** option.
- Select ***Connect manually*** if you always want to establish and end the connection to the Internet manually. If you subscribe to a time-based service this will save you high connection charges. How to establish a connection manually is described on page 77.

→ Click ***Test Settings*** to check the Internet connection. The device will attempt to connect to the Internet. Any Internet connection already in existence will be closed first.

This displays information on the tests that have been carried out and their results.

You will then be returned to the ***Internet Connection*** screen. If necessary, you can now correct your entries.

→ If the test was successful, click ***OK*** to apply the settings.

PPPoE pass-through

If you activate the ***PPPoE pass-through*** function, a PC in the network can connect to the Internet via its own connection ID. The router puts these connections through.

→ In the ***Advanced Settings*** – ***Internet*** menu, select the entry ***Internet Connection***.

→ Select ***On*** to activate ***PPPoE pass-through***.

→ Click ***OK*** to apply the settings.

Using UPnP (Universal Plug & Play)

PCs with UPnP (Universal Plug & Play) can offer their own network services and automatically use services offered on the network.

> **Note:**
> Check whether the UPnP function has been installed in your PC's operating system. If not, you may have to install your operating system's UPnP components. Please consult your PC operating instructions.

As soon as you have installed UPnP in the operating system of a PC and activated it on the router, applications on this PC (e.g. Microsoft Messenger) can communicate via the Internet without you needing to grant explicit authorisation. In this case, the router automatically implements Port Forwarding, see page 59, thereby facilitating communication via the Internet.

You will see a symbol for your Gigaset SE366 WLAN in the taskbar on the PC on which UPnP is installed. Windows XP systems will also include the icon under its Network Connections. Clicking this icon opens the Gigaset SE366 WLAN's configuration screens.

→ In the ***Advanced Settings*** – ***Internet*** menu, select the entry ***Internet Connection***.

→ Select ***UPnP***.

> **Note:**
> When the UPnP function is active, system applications can assign and use Ports on a PC. This can be a security risk.

→ Click ***OK*** to apply the settings.

IGMP proxy server

IGMP (Internet Group Management Protocol) enables a PC to report its membership of a multicast group to other PCs over the Internet. With multicasting, a PC can send content on the Internet to several other PCs that have registered an interest in the first computer's data and information.

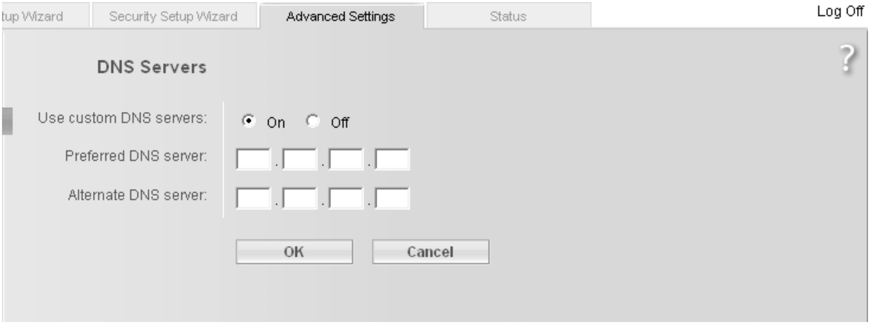
→ Activate ***IGMP proxy server*** if you wish to use this function.

DNS server

DNS is a decentralised service that assigns PC names or Internet addresses (Domain names) and IP addresses to one another. A DNS server has to administer this information for each server or each LAN with an Internet connection.

Normally your Internet provider supplies you with a DNS server, which makes this assignment when the connection to the Internet is set up. If necessary, you can define the DNS server to be used for Internet connections manually.

→ In the ***Advanced Settings*** – ***Internet*** – ***Internet Connection*** menu, select the entry ***DNS Servers***.



DNS Servers

Use custom DNS servers: ● On ○ Off

Preferred DNS server: □ . □ . □ . □

Alternate DNS server: □ . □ . □ . □

→ Activate the ***Use custom DNS servers*** function by selecting ***On***.

→ Enter the IP addresses for your ***Preferred DNS server*** and ***Alternate DNS server***.

→ Click ***OK*** to apply the settings.

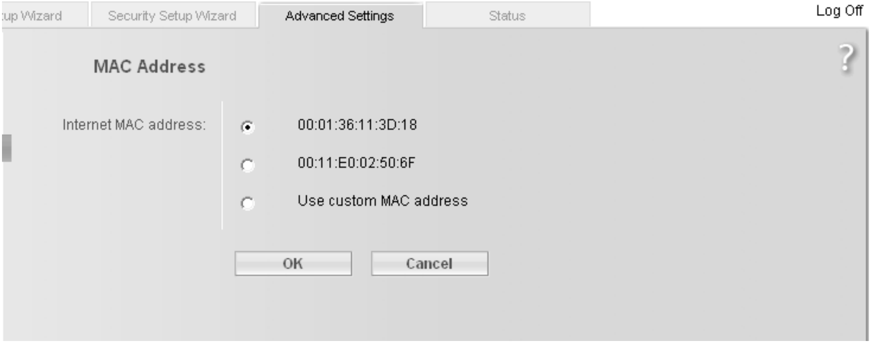
MAC address

If you had Internet access through the same Internet provider before connecting the Gigaset SE366 WLAN, then it is possible that the MAC address of one of your PCs was used for registration when access was configured. In this case, you must either replace the current MAC address with the MAC address registered with the Internet provider or ask your Internet provider to register a new MAC address for your account.

Carry out the following steps:

→ Connect a PC to the Gigaset SE366 WLAN and open the configuration environment.

→ In the ***Advanced Settings*** – ***Internet*** – ***Internet Connection*** menu, select the entry ***MAC address***.



MAC Address

Internet MAC address:

● 00:01:36:11:3D:18

○ 00:11:E0:02:50:6F

○ Use custom MAC address

→ Select the MAC address that is to apply to the Internet connection:

- ***Use default device MAC address***: You can leave this default setting if the MAC address of the Gigaset SE366 WLAN is used to connect to the Internet.
- ***Use MAC address of this PC***: Select this option if the MAC address of the currently connected PC was previously registered for connecting to the Internet or if you have re-registered the MAC address of the PC on which you are currently working.
- ***Use custom MAC address***: Select this option if you have asked your Internet provider to register a new MAC address and this is not the MAC address of the PC on which you are currently carrying out the configuration.

→ Click ***OK*** to apply the settings.

Firewall

The firewall functions of the Gigaset SE366 WLAN include various security functions for your local network.

You can:

- protect your network against hacker attacks (see below),
- block individual PCs' access to individual services or Internet sites(see page 53).

The firewall functions for the Gigaset SE366 WLAN are activated and configured in the factory. If you wish to deactivate the firewall, carry out the following steps:

→ In the ***Advanced Settings*** – ***Internet*** menu, select the entry ***Firewall***.

→ Select the required option.

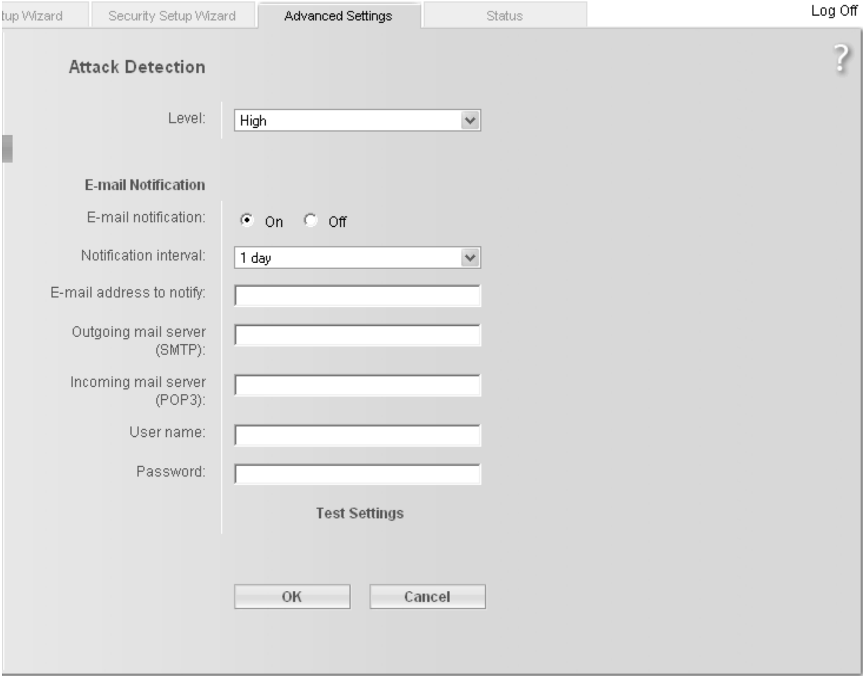
→ Click ***OK*** to apply the settings.

Attack detection

If the firewall functions of your Gigaset SE366 WLAN are activated, the device monitors and limits access by incoming data traffic via the Internet connection with a function called Stateful Packet Inspection (SPI). This allows the Gigaset SE366 WLAN to identify and block certain types of attack from the network, e.g. Denial of Service (DoS). DoS attacks are aimed at devices and networks with Internet connections. The aim is not so much to steal data but to paralyse the computer or network so that network resources are no longer available. A typical hacker attack involves a remote computer claiming to be the paralysed device in order to take its place and receive the data intended for it.

You can use the Attack Detection function to change the standard firewall settings and arrange to be notified by email about any attempted hacker attacks.

→ In the ***Advanced Settings*** – ***Internet*** – ***Firewall*** menu, select ***Attack Detection***.



Attack Detection

Level: High

E-mail Notification

E-mail notification: ● On ○ Off

Notification interval: 1 day

E-mail address to notify:

Outgoing mail server (SMTP):

Incoming mail server (POP3):

User name:

Password:

➜ Select the security level for the firewall.

The default level ***High*** offers you maximum security coupled with potentially limited functionality for individual applications.

- The ***Medium*** level offers high security but may involve functionality restrictions.
- The ***Low*** level offers you maximum functionality but may involve reduced security.

E-mail notification of a hacker attack

You can choose to be informed by e-mail about any hacker attack.

➜ Enter the following in the dialogue fields:

- Select the ***Notification interval***, i.e. at what intervals you wish to be informed about hacker attacks. If hacker attacks have been identified and blocked in the intervening period, you will receive a summary of the events.
- ***E-mail address to notify***: Enter the e-mail address to which the notifications are to be sent.
- ***Outgoing mail server (SMTP)***: Enter the address of the outgoing mail server through which your device can send you the notifications.
- ***Incoming mail server (POP3)***: If your outgoing mail server demands authentication via POP3 before e-mails can be sent, enter the address of the outgoing mail server here.
- Enter your ***User name*** and the relevant ***Password***.

➜ Click ***Test Settings*** to check the details for e-mail notification.

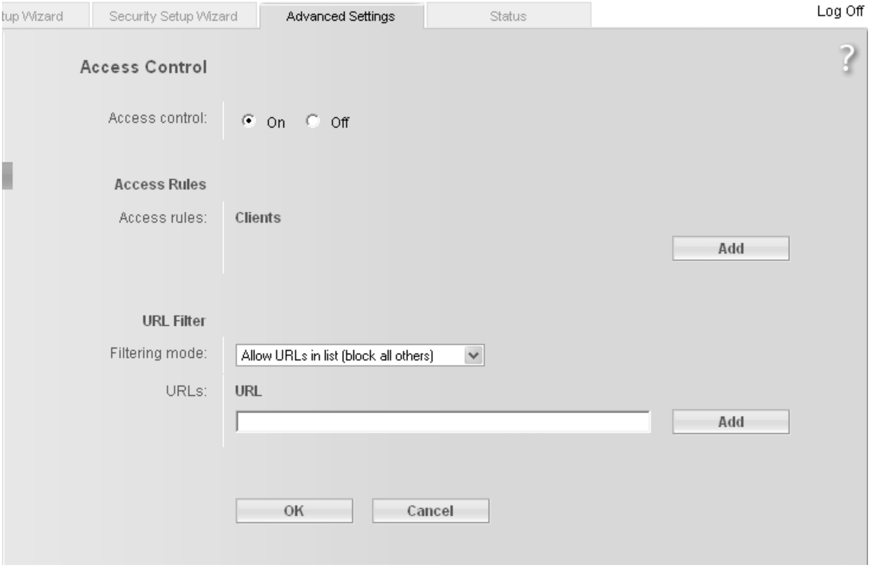
➜ Click ***OK*** to apply the settings.

Setting up access control to the Internet

The ***Access Control*** function allows you to block access to various Internet services for one or more PCs.

→ In the ***Advanced Settings*** – ***Internet*** – ***Firewall*** menu, select ***Access Control***.

→ Activate the ***Access Control*** function via the option ***On***.



Access Control

Access control: ● On ○ Off

Access Rules

Access rules: Clients

URL Filter

Filtering mode: Allow URLs in list (block all others)

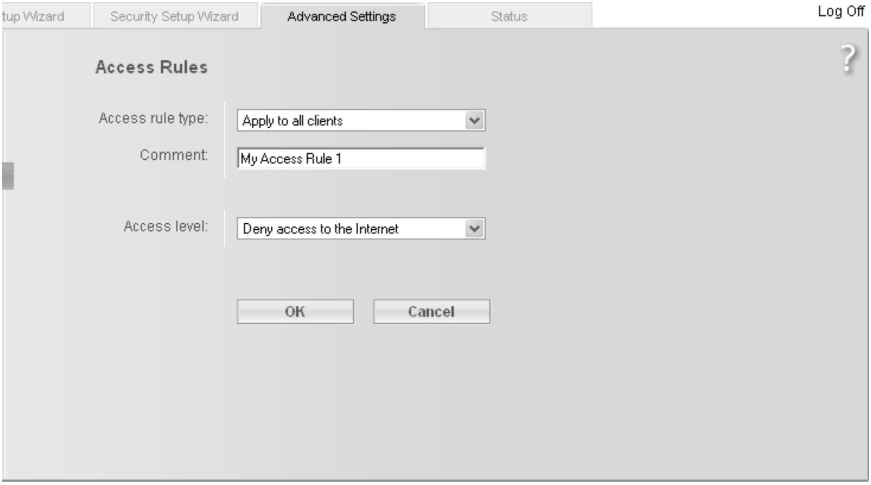
URLs: URL

You have the following setting options for ***Access Control***:

Access Rules

You can limit access to the Internet for all or for certain clients in your local network. You can allow or block access to URLs and services.

→ Click ***Edit*** to create an access rule.



Access Rules

Access rule type: Apply to all clients

Comment: My Access Rule 1

Access level: Deny access to the Internet

→ Select the ***Access rule type*** from the list:

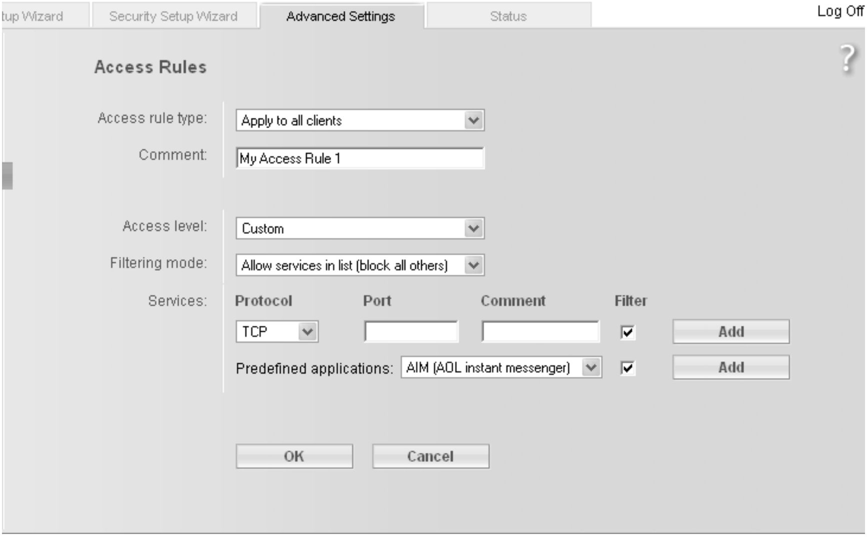
- ***Apply to all clients***: The rule applies to all PCs in your network.
- ***Specify IP address range***: You select the PCs to which the rule is to apply by entering an IP address block.
- ***Specify IP address*** or ***Specify MAC address***: The rule applies to a PC you select via its IP address or MAC address.

→ Enter a name for the ***Description*** of the access rule.

→ Define the ***Access level***.
You can apply ***Deny access to the Internet***, ***Allow web browsing with URL filter***, ***Allow web browsing*** or make user-defined settings.

If you select ***Allow web browsing with URL filter***, you must define the URL filter (see page 56).

If you select ***Custom***, you have the following possibilities:



Access Rules

Access rule type: Apply to all clients

Comment: My Access Rule 1

Access level: Custom

Filtering mode: Allow services in list (block all others)

Services:

Protocol	Port	Comment	Filter
TCP			☑

Predefined applications: AIM (AOL instant messenger) ☑

- In ***Filtering mode***, define whether the services you select are to be allowed or blocked.
- Select the ***Services*** you wish to allow or block.

  Select the ***Protocol*** and enter the appropriate ***Port*** (a single port number, several individual port numbers separated by commas, port blocks consisting of two port numbers separated by a hyphen, or any combination of these, e.g. **`80,90-140,180`**). The displayed ***Description*** helps you to identify different services.
- Activate the ***Filter*** option to use the service concerned for the service filter.
- You can also select services from the ***Predefined applications*** list.
- Click ***Delete*** to delete an entry. Click ***Add*** to create a new entry with the entered data or for the selected predefined application.

→ Click ***OK*** to apply the settings.

URL filter

The URL filter allows you to block access to certain Internet sites or Internet domains, or to limit accesses to certain Internet sites. Once you have entered the relevant URLs you can then create access rules that apply the URL filter to the selected clients in your network.

→ In the ***Advanced Settings*** – ***Internet*** – ***Firewall*** menu, select ***Access Control***.

→ Select ***Filtering mode***, i.e. whether you wish to allow or block access to the URLs in the list.

→ Enter the required URL in the field.

→ Click ***Delete*** to delete an entry. Click ***Add*** to create a new entry.

→ Click ***OK*** to apply the settings.

Setting up the NAT function

Your Gigaset SE366 WLAN comes provided with the NAT (Network Address Translation) function. With address translation, several users on your local network can access the Internet via one or more public IP addresses. In the default setting, all local IP addresses are mapped to your router's public IP address.

One property of NAT is that data from the Internet is not allowed into your local network unless it has been explicitly requested by one of the PCs on that network. Most Internet applications run behind the NAT firewall without any problems. If you request Internet pages, for example, or send and receive e-mails, the request for data from the Internet comes from a PC on the local network and the router allows the data through. The router opens exactly **one** port for the application. A port is an internal PC address through which the data is exchanged between a server on the Internet and a client on a PC in the local network. Communicating via a port follows the rules of a specific protocol (TCP or UDP).

If an external application tries to send a call to a PC within the local network, the router will block it. There is no open port via which the data could enter the local network.

Some applications, such as games on the Internet, require several links, i.e. several ports so that the players can communicate with each other. In addition, these applications must also be permitted to send requests from other users on the Internet to the user on the local network. Initially, these applications will not work if Network Address Translation (NAT) is activated.

Using port forwarding (the forwarding of requests to specific ports) you make the router forward requests from the Internet for a certain service, e.g a game, to the appropriate port or ports on the PC on which the game is running.

Port triggering is a specific variant of port forwarding. Unlike port forwarding, in this case the Gigaset SE366 WLAN forwards data from the set port block to the PC which has previously sent data to the Internet via a certain port (trigger port). This means that permission for data transfer is not tied to one specific PC in your network, but only to the port numbers of the required Internet service.

Where configuration is concerned, this means:

- You have to define a so-called trigger port for the application and also the protocol (TCP or UDP) that this port uses. To this trigger port you then assign the public ports that have to be opened for the application.
- The router checks all outgoing data for port number and protocol. If it recognises a match of port and protocol to a defined trigger port, then it will open the assigned public ports and notes the IP address of the PC that sent the data. If data comes back from the Internet via one of these public ports, it allows the data through and routes it to the right PC. A trigger event always comes from a PC within the local network. If a trigger port is addressed from outside, it is simply ignored by the router.

Note:

- An application that is configured for port triggering can only be run by one user in the local network at a time.
- As long as the public ports are open, they can be used by unauthorised persons to gain access to a PC in the local network.

When the Gigaset SE366 WLAN is delivered, the NAT function (Network Address Translation) is activated, i.e. all IP addresses of PCs in the local network are mapped to the router's public IP address when accessing the Internet.

You can use the NAT settings for the Gigaset SE366 WLAN to

- set up port triggering for special applications (see page 58),
- set up the Gigaset SE366 WLAN as a virtual server by configuring Port Forwarding (see page 59),
- open the firewall for selected PCs (see page 60).

Note:

For the functions described below you must make sure that the IP addresses of the PCs do not change. If the IP addresses of the PCs are assigned via the DHCP server of the Gigaset SE366 WLAN, you must select the option ***Never expires*** for the settings on the ***Local Network*** screen for ***Lease time*** (see page 64) or assign static IP addresses for the PCs.

You can activate or deactivate the NAT function (default setting: NAT function is activated).

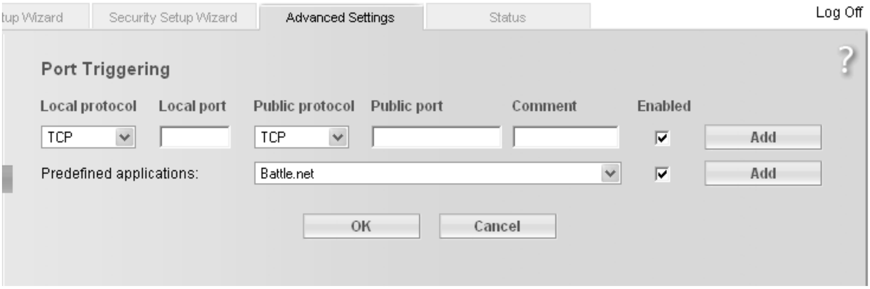
→ In the ***Advanced Settings*** – ***Internet*** menu, select ***Address Translation (NAT)*** and mark the required option.

Port triggering

If you configure port triggering for a certain application, define a so-called trigger port and the protocol (TCP or UDP) this port uses. You then assign the public ports that have to be opened for the application to this trigger port.

You can select known Internet services for this or assign ports or blocks of ports manually.

→ To set up port triggering for a service, select ***Port Triggering*** in the ***Address Translation (NAT)*** menu.



Port Triggering

Local protocol	Local port	Public protocol	Public port	Comment	Enabled	
TCP		TCP			☑	Add
Predefined applications:		Battle.net			☑	Add

→ Select the required application from the ***Predefined applications*** list.

→ Click the ***Add*** button. The data for the required service is entered on the screen.

→ Select the option in the ***Enabled*** column.

If the application you require is not in the list, you must enter the relevant data on the screen manually:

→ ***Local protocol***: Select the protocol that is to be monitored for outgoing traffic.

→ ***Local port***: Enter the port that is to be monitored for outgoing traffic.

→ ***Public protocol***: Select the protocol that is to be allowed for incoming data traffic.

→ ***Public port***: Enter the port that is to be opened for incoming data traffic.

Note:
You can enter a single port number, several individual port numbers separated by commas, port blocks consisting of two port numbers separated by a hyphen, or any combination of these, e.g. **`80,90-140,180`**.

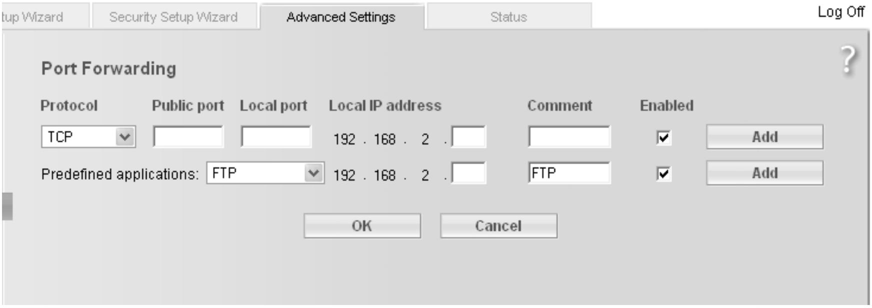
- → ***Description***: Enter a description to help you identify different entries.
- → Select the option in the ***Enabled*** column.
- → Click the ***Delete*** button to delete an entry. Click the ***Add*** button to add a new entry.
- → Click ***OK*** to apply the settings.

Port Forwarding

If you configure Port Forwarding, the Gigaset SE366 WLAN outwardly assumes the role of the server. It receives requests from remote users under its public IP address and automatically redirects them to local PCs. The private IP addresses of the servers on the local network remain protected.

Internet services are addressed via defined port numbers. The Gigaset SE366 WLAN needs a mapping table of the port numbers to redirect the service requests to the server that actually provides the service. For this, Port Forwarding has to be configured.

- → To set up port forwarding for a service, select ***Port Forwarding*** in the ***Address Translation (NAT)*** menu.



Port Forwarding

Protocol	Public port	Local port	Local IP address	Comment	Enabled	
TCP			192 . 168 . 2 .		☑	Add
Predefined applications: FTP			192 . 168 . 2 .	FTP	☑	Add

- → Select the required application from the ***Predefined applications*** list.
- → Click the ***Add*** button. The data for the required service is entered on the screen.
- → Select the option in the ***Enabled*** column.

If the application you require is not in the list, you must enter the relevant data on the screen manually:

- → Select the protocol for the service you are providing from the ***Protocol*** list.
- → Under ***Public port***, enter the port number of the service you are providing.
- → In the ***Local port*** field, enter the internal port number to which service requests are to be forwarded.

> **Note:**
>
> You can enter a single port number or a port block consisting of two port numbers separated by a hyphen, e.g. **`80`** or **`90-140`**.

→ In the ***Local IP address*** field, enter the IP address of the PC which provides the service.

Example: The Web server has been configured to react to requests on port 8080. However, requests from websites enter by port 80 (default setting). If you add the PC to the forwarding table and define port 80 as the public port and port 8080 as an internal port, all requests from the Internet are diverted to the service with port number 80 on the Web server of the PC you have defined with port 8080.

→ Click ***Add***.

→ Click ***Delete*** if you wish to delete the data in the relevant line again.

→ Select the option in the ***Enabled*** column.

→ Click ***OK*** to apply the settings.

Opening the firewall for selected PCs (Exposed Host)

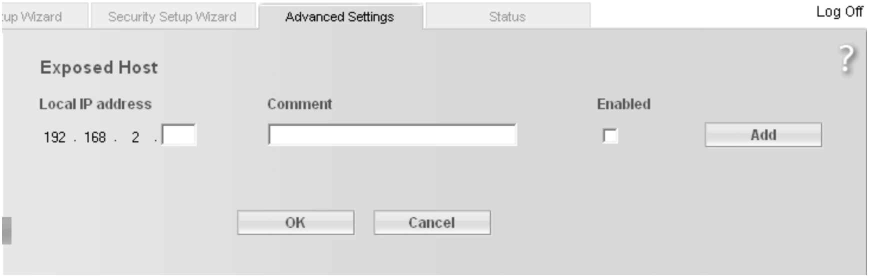
You can set up a client as an exposed host in your local network. Your device will then forward all incoming data traffic from the Internet to this client. This will enable you, for example, to operate your own Web server on one of the clients in your local network and make it accessible to Internet users.

As an exposed host, your local client is directly visible on the Internet and therefore particularly exposed to risk (e.g. from hacker attacks). You should only activate this function where it is absolutely necessary (e.g. to operate a Web server) and where other functions (e.g. port forwarding) are not adequate. In this case you should take appropriate measures on the clients concerned.

Note:

Only one PC per public IP address can be set up as Exposed Host (see also the section entitled "Port Forwarding" on page 59.

→ To set up a PC as an Exposed Host, select ***Exposed Host*** in the ***Address Translation (NAT)*** menu.



Exposed Host

Local IP address: 192 . 168 . 2 .

Comment:

Enabled: □

→ Enter the ***Local IP address*** of the PC that is to be enabled as Exposed Host.

→ Enter a name for the PC in the ***Comment*** field.

→ Enable the entry by selecting the option.

→ Click ***Add*** to add the entry to the list.

→ Click ***Delete*** to delete the entry from the list.

→ Click ***OK*** to apply the settings.

Dynamic DNS

Any service you provide on the Internet can be accessed via a Domain name. Your router's Public IP address is assigned to this domain name. If your Internet Service Provider for your local network's WAN connection assigns the IP address dynamically, the IP address of the router may change. The assignment to the domain name will no longer be valid and your service will no longer be available.

In this case you must ensure that the assignment of the IP address to the domain name is constantly updated. This is handled by the dynamic DNS service (DynDNS). You can use the DynDNS service to assign your Gigaset SE366 WLAN an individual static domain name on the Internet even if it does not have a static IP address.

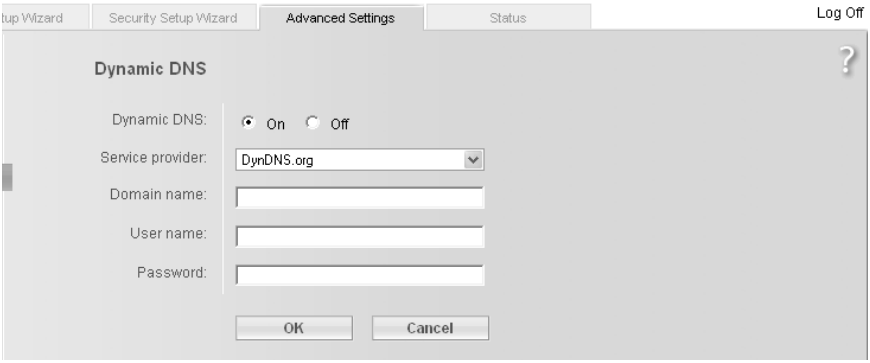
There are various providers on the Internet who offer a free DynDNS service. The Gigaset SE366 WLAN uses the DynDNS service from **DynDNS.org** and from TZO.org. If you use this DynDNS provider's service, then your service can be reached on the Internet as a subdomain of one of this provider's domains.

If you have activated the device's DynDNS function, it will monitor its public IP address. When this changes, it sets up a connection to the Internet site and updates its IP address there.

Note:

You will have to open an account with the provider before you can use the Gigaset SE366 WLAN's DynDNS function. Follow the instructions on the provider's web site. Enter the user data during configuration of the router.

→ To use the router's DynDNS function, select *Dynamic DNS* in the *Advanced Settings – Internet* menu.



Dynamic DNS

Dynamic DNS: ● On ○ Off

Service provider: DynDNS.org

Domain name:

User name:

Password:

→ Activate the *Dynamic DNS* function.

→ From the *Service provider* list, select the service offering dynamic DNS (DynDNS.org or TZO.com).

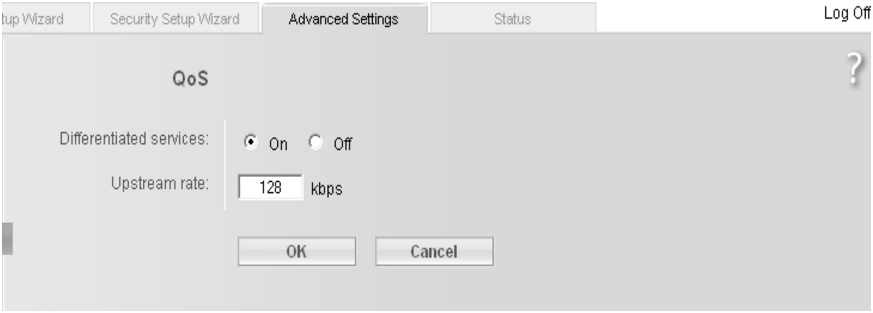
→ Enter the *Domain name*, *User name* and *Password*. You will have received the necessary information when registering with your *Service provider*.

→ Click *OK* to apply the settings.

QoS (Quality of Service)

Many communication and multimedia applications require high speed and large bandwidths to transfer data between the local area network and the Internet. However, for many applications there is often only one Internet connection with limited capacity available. *QoS* (Quality of Service) divides this capacity between the different applications and provides undelayed, continuous data transfer where data packets with higher priority are given transmission preference.

→ In the *Advanced Settings – Internet* menu, select the entry *QoS*.



QoS

Differentiated services: ● On ○ Off

Upstream rate: 128 kbps

→ Activate ***Differentiated services***, i.e. the prioritisation of certain services for data transfer between your network and the Internet.

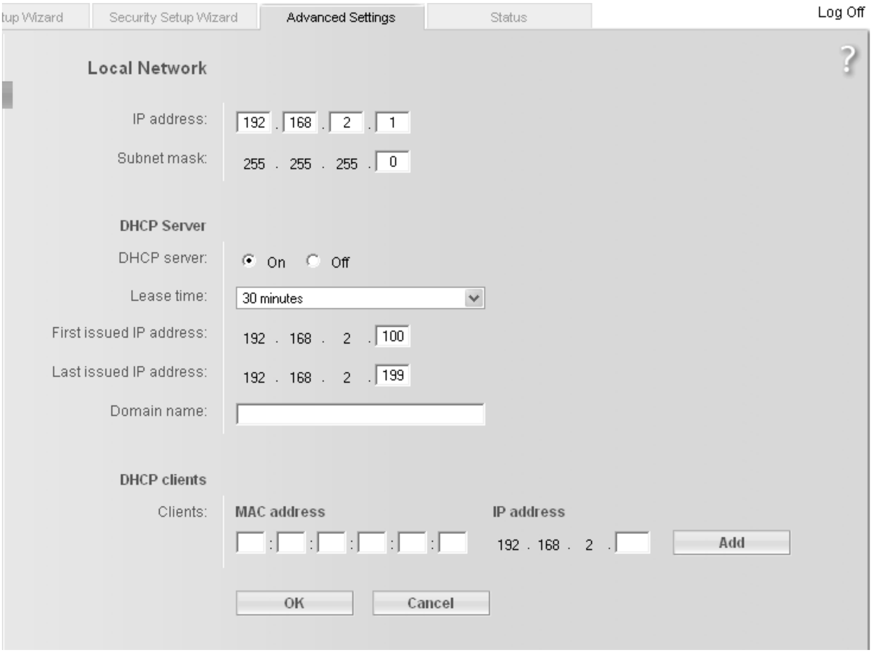
→ In the field next to ***Upstream rate***, enter the maximum speed of your DSL line for sending data into the Internet. The speed is specified in the contract with your Internet provider.

→ Click ***OK*** to accept the changes.

LAN configuration

You can use the LAN configuration to define an IP address for the Gigaset SE366 WLAN and configure the DHCP server.

→ Select ***Advanced Settings*** – ***Local Network***.



Local Network

IP address: 192 . 168 . 2 . 1

Subnet mask: 255 . 255 . 255 . 0

DHCP Server

DHCP server: ● On ○ Off

Lease time: 30 minutes

First issued IP address: 192 . 168 . 2 . 100

Last issued IP address: 192 . 168 . 2 . 199

Domain name:

DHCP clients

Clients: MAC address IP address

□ : □ : □ : □ : □ : □ 192 . 168 . 2 . □

Defining the private IP address for the Gigaset SE366 WLAN

On this screen you can change the device's IP address. The default IP address is 192.168.2.1. This is the Gigaset SE366 WLAN's Private IP address. It is the address under which the device can be reached on the local network. The address can be freely assigned from the block of available addresses. The IP address under which the Gigaset SE366 WLAN can be reached from outside is assigned by the Internet Service Provider.

→ If you want to assign the Gigaset SE366 WLAN a different IP address, enter it in the fields next to ***IP address***.

→ If you want to use a different subnet mask, enter it in the ***Subnet mask*** field. Only the last field can be changed.

We recommend using an address from a block that is reserved for private use. This address block is 192.168.1.1 – 192.168.255.254.

Note:

New settings only take effect after rebooting the Gigaset SE366 WLAN. If necessary, reconfigure the IP address on your PC (including one that is statically assigned) so that it matches the new configuration.

Configuring the DHCP server

The Gigaset SE366 WLAN has a DHCP server, which is enabled on delivery. As a result, the IP addresses of the PCs are automatically assigned by the Gigaset SE366 WLAN.

Note:

◆ If the Gigaset SE366 WLAN's DHCP server is activated, you can configure the network setting on the PC so that the option ***Obtain an IP address automatically*** is set. To find out how to do this, please refer to the document “Configuring the local network” on the CD.

◆ If you deactivate the DHCP server, you will have to assign a static IP address for the PCs via the network settings.

→ To activate the DHCP server, select ***On***.

→ If the DHCP server is active, you can define a ***Lease time***. The Lease time determines the period for which the PCs keep the IP addresses assigned to them without any change.

Note:

If you select the ***Never expires*** option, the IP addresses are never changed. You must select this option if you want to make NAT or firewall settings using the IP addresses of the PCs, or else you must assign these PCs static IP addresses.

→ Define the range of IP addresses which the Gigaset SE366 WLAN should use to automatically assign IP addresses to PCs. Define the ***First issued IP address*** and the ***Last issued IP address***.

→ You can define the name of a domain (Windows workgroup) in the ***Domain name*** field.

Assigning static IP addresses to individual PCs

Even if you have activated the DHCP server you can still assign a static IP address to individual PCs (e.g. when setting up these PCs for NAT functions).

→ Enter the ***MAC address*** and the name of the PC in the ***Device name*** field.

→ Enter the ***IP address*** you wish to assign to the PC in the field below.

→ Click ***Add*** to add the entry to the list.

→ Click ***Delete*** to delete the entry from the list.

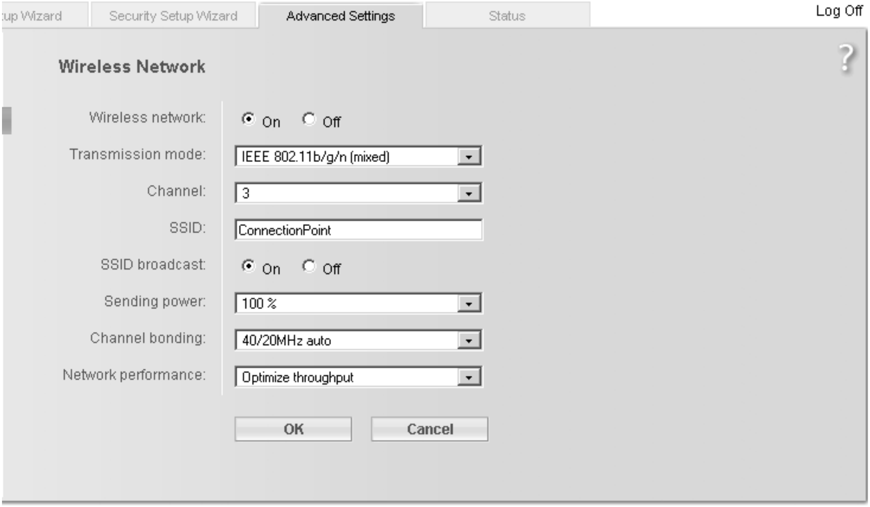
→ Click ***OK*** to apply the settings.

Configuration for wireless connections

If PCs communicate wirelessly via the Gigaset SE366 WLAN, you should take steps to enhance the security of your wireless network. You make this configuration via the ***Advanced Settings*** – ***Wireless Network*** menu. Here you can

- activate the Gigaset SE366 WLAN's wireless module (see below),
- set the channel and SSID (see page 66),
- activate and configure WPS (see page 68),
- set Encryption for wireless traffic (see page 69),
- restrict access to the Gigaset SE366 WLAN's LAN (see page 74),
- configure the Gigaset SE366 WLAN's repeater function (see page 75).

→ In the ***Advanced Settings*** menu, select ***Wireless Network***.



Wireless Network

Wireless network:	● On ○ Off
Transmission mode:	IEEE 802.11b/g/n (mixed)
Channel:	3
SSID:	ConnectionPoint
SSID broadcast:	● On ○ Off
Sending power:	100 %
Channel bonding:	40/20MHz auto
Network performance:	Optimize throughput

→ Select the ***On*** option for ***Wireless Network*** (default setting).

Devices can only log in wirelessly if the Gigaset SE366 WLAN's wireless module is activated.

You can now make the settings for your wireless network.

Transmission mode

The transmission mode defines which IEEE standard you use to transmit data in your network. IEEE 802.11g permits data transfer up to 54 Mbps, IEEE 802.11b up to 11 Mbps. In contrast, IEEE 802.11n (draft, see page 15) reaches a transmission rate of up to 300 Mbps.

→ For the best possible data transfer rates in your network select ***IEEE 802.11b/g/n (mixed)***.

SSID

For the wireless network components to communicate with each other, they must have the same SSID (Service Set Identifier).

Note:

If you have already activated WPS (see page 68), the generated SSID is displayed on this screen. You should not change this SSID here manually. Otherwise, the registered clients will no longer have access to your wireless network.

On delivery, the Gigaset SE366 WLAN's default SSID is **ConnectionPoint**. If you are not using WPS, you should change this SSID for security reasons.

For security reasons you should deactivate SSID broadcast (see page 67).

To change the SSID manually, enter a character string of your choice. The SSID is case sensitive. It can be up to 32 alphanumeric characters long.

Note:

The connection to the wireless network adapters will be interrupted until you enter the new SSID on them as well.

Channel

All the clients in your network use the set radio channel for wireless data transmission. You can choose between various channels, depending on your current location.

→ Select the channel for transmitting the data.

SSID broadcast

If this option is enabled (default setting), the Gigaset SE366 WLAN will send the SSID with all data transmissions and your Gigaset SE366 WLAN's SSID will be displayed on PCs that have a wireless network adapter. In this case, eavesdroppers could use the SSID to gain access to your local network.

If you disable ***SSID broadcast***, your Gigaset SE366 WLAN's SSID will not be displayed. This increases protection against unauthorised access to your wireless network. However, you must make a note of the SSID. You will need it to log in to your PC.

→ Select the ***Off*** option to deactivate ***SSID broadcast***.

Sending power

→ Select the required sending power for your device.

We recommend that you select a sending power with a range to suit the spatial environment of your local network. A range that is much greater makes it easier to eavesdrop on your wireless data transmission.

Channel bonding

You can only use ***Channel bonding*** if this function is supported by at least one client in your wireless network. For the best possible data transfer rates, all clients in your wireless LAN should support ***Channel bonding***.

→ Select an option for ***Channel bonding*** from the list: ***20 MHz***, ***40 MHz*** or ***40/20 MHz Auto*** (default).

Network performance

You can optimise network performance in the following ways:

- ***Optimize throughput***
  maximises the data transmission rate in your network and ensures that data traffic is transmitted immediately.
- ***Optimize power saving***
  optimises power consumption in order to extend standby times for mobile devices in your network, e.g. notebooks, PDAs and WLAN handsets.
- ***Custom***
  This allows you to adjust the netwoek performance to suit your needs on the basis of the following items:
  - ***Beacon interval*** defines the interval between two Beacons.
    Measured in milliseconds, default = 100 msecs.
  - ***DTIM interval*** defines the interval between two DTIMs for devices in power-saving mode.
    Measured in number of beacons, default = 2 beacons.

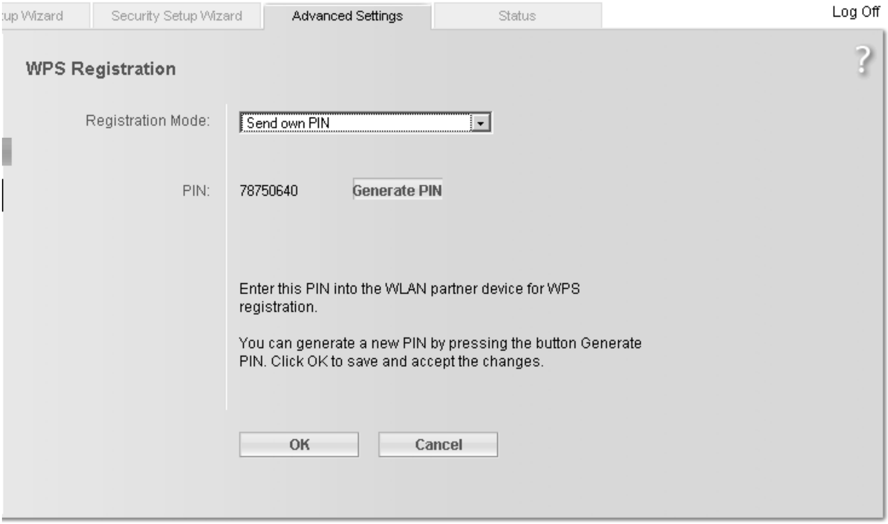
→ Choose the desired ***Network performance***.

Configuring WPS

Wifi Protected Setup (WPS) makes it easier to establish a wireless network. Devices equipped with WPS are able to create and synchonise an SSID and a WPA key (pre-shared key) automatically.

All you need to do to establish a secure wireless connection is press the registration button and click once in the user interface of the client. For further information, see section "WPS" on page 13.

→ In the ***Wireless Network*** menu, choose ***WPS Registration***.



Registration Mode: Send own PIN

PIN: 78750640

Enter this PIN into the WLAN partner device for WPS registration.

You can generate a new PIN by pressing the button Generate PIN. Click OK to save and accept the changes.

→ Choose the desired ***Registration Mode***:

- ***Push Button***

  Click ***OK*** to start the WPS registration.

  This function corresponds to pressing the **Registration** button on the device’s back panel.

  After starting the WPS registration, the device searches for a WPS client in range. Any WPS client in range that activates its WPS function within two minutes gets the Gigaset SE366 WLAN security data (SSID and pre-shared key) and is thereby registered.

  The registration progress is shown in the window.

  You can also follow the registration process via the LED display (see page 19).

- ***Send own PIN***

  An automatically generated PIN is shown.

  If you want to create a new PIN, click ***Generate PIN***. Please note that any devices that may be connected with the old PIN no longer have access to the Gigaset SE366 WLAN.

  Click OK to activate your settings.

Enter the generated PIN on all WLAN partner devices that are to establish a connection.

– ***Enter partner device PIN***

  You would only use this option if the PIN of another device is being used in your WLAN. Enter the PIN of the WLAN partner device and click ***OK*** to activate your settings. This PIN must be used by all WLAN partners for logging on to the Gigaset SE366 WLAN.

Note:

If you have activated access control via the MAC address filter, only clients already included in the MAC address list can register via WPS.

Setting encryption

You should activate data encryption to protect your wireless local network against eavesdropping from outside or to prevent unauthorised access to your data.

If you send data over wireless channels, we recommend that you activate encryption (WEP or WPA) on your wireless network components.

Note:

If you have already performed WPS registration, WPA2-PSK/WPA-PSK encryption is activated. The following description is only valid if you are not using WPS.

➙ In the ***Wireless Network*** menu, select ***Encryption***.

The following security mechanisms are currently available:

◆ WPA2-PSK and WPA2-PSK / WPA-PSK (see page 70)

◆ WPA2 and WPA2 / WPA with authentication server (see page 70)

◆ WEP encryption (Wired Equivalent Privacy), (see page 71).

WPA2-PSK and WPA2-PSK / WPA-PSK

Note:

If you have already performed WPS registration (see page 13 or page 68), you will see the generated pre-shared key on this screen. You can change the encryption here if you don’t want to use WPS. In this case, you also have to configure all wireless network adapters manually.

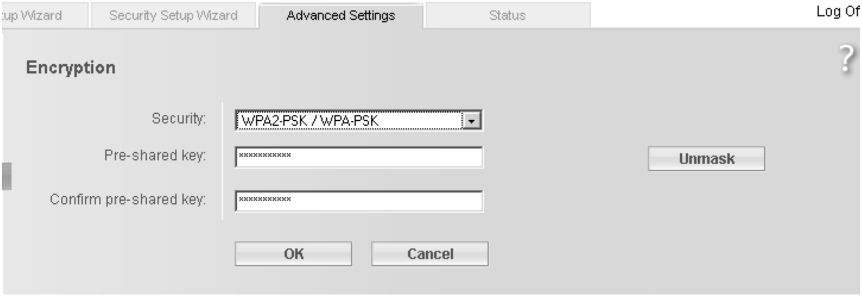
If you performed manual encryption first and then performed WPS registration, the manual encryption data is overwritten. You then have to register all wireless network adapters via WPS or manually re-enter the encryption generated with WPS on the network adapters.

WPA with pre-shared key (WPA-PSK)

WPA-PSK is a special WPA mode that provides encryption protection for users at home and in small companies without a company authentication server. Encryption keys are automatically generated with the pre-shared key and automatically changed (rekeying) and authenticated between the devices after a certain period of time (Rekey interval).

Which standard of encryption you can choose depends on the components in your wireless network. Every PC (network adapter) that requires access to a wireless network protected by WPA must also support WPA. To find out whether and how you can use WPA on your PC, read your network adapter's operating instructions. If all components support WPA2, select the ***WPA2-PSK*** option. If you are using network adapters that only support WPA, select the ***WPA2-PSK / WPA-PSK*** option. The entries described below are the same for both options.

→ Select the required option in the ***Security*** field.



Encryption

Security: WPA2-PSK / WPA-PSK

Pre-shared key: ************

Confirm pre-shared key: ************

→ Enter a key in the ***Pre-shared key*** field (up to 63 alphanumeric characters) and confirm it by entering it again.

→ By clicking the ***Unmask*** button, a message showing the pre-shared key is output in readable characters.

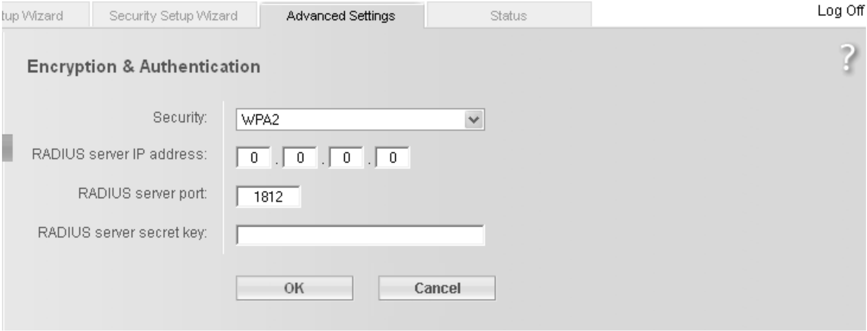
→ Apply the settings by clicking ***OK***.

WPA2 and WPA with authentication server

In large networks (e.g. in business enterprises) WPA enables the use of an additional authentication service. In this case, user access is controlled by user accounts and passwords, in addition to WPA encryption. A RADIUS server acts as an authentication server. You can select the new standard ***WPA2*** if this is supported by all components in your wireless network, or select ***WPA2 / WPA*** if you are using devices that only support WPA.

You cannot use WPA2 / WPA together with WPS.

→ Select the required option in the ***Security*** field.



Encryption & Authentication

Security: WPA2

RADIUS server IP address: 0 . 0 . 0 . 0

RADIUS server port: 1812

RADIUS server secret key:

→ Enter the IP address of the RADIUS server in the ***RADIUS server IP address*** field.

→ Enter the port of the RADIUS server in the ***RADIUS server port*** field.

→ In the ***RADIUS server secret key*** field, enter a keyword that complies with the conventions of the RADIUS server and that is to be used by the server for authentication.

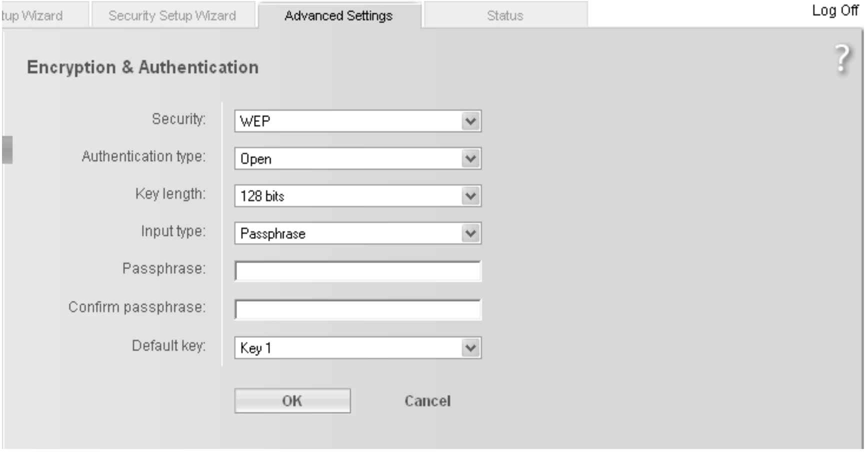
→ Click ***OK*** to apply the settings.

WEP encryption

If WPA is not supported by all components in your wireless network, we advise you to activate WEP Encryption on your wireless network components.

Note:
You cannot use WEP together with WPS.

→ In the ***Security*** field, select the ***WEP*** option.



Encryption & Authentication

Security: WEP

Authentication type: Open

Key length: 128 bits

Input type: Passphrase

Passphrase:

Confirm passphrase:

Default key: Key 1

→ Select the ***Authentication type***:

– Select ***Shared*** if you want each client to log in to the network with a specified key.

– Select ***Open*** to permit data transfer within your wireless network without using a key.

You can choose either the standard 64-bit keys or the more robust 128-bit keys for encryption. The keys are generated in hexadecimal or ASCII format. You must use the same keys for encryption and decryption for both the Gigaset SE366 WLAN and all your wireless network adapters.

→ Select the ***Key length***: 64 or 128-bit.

→ Select the ***Input type***, i.e. whether you wish to enter the key manually or have it generated automatically by means of a ***Passphrase***.

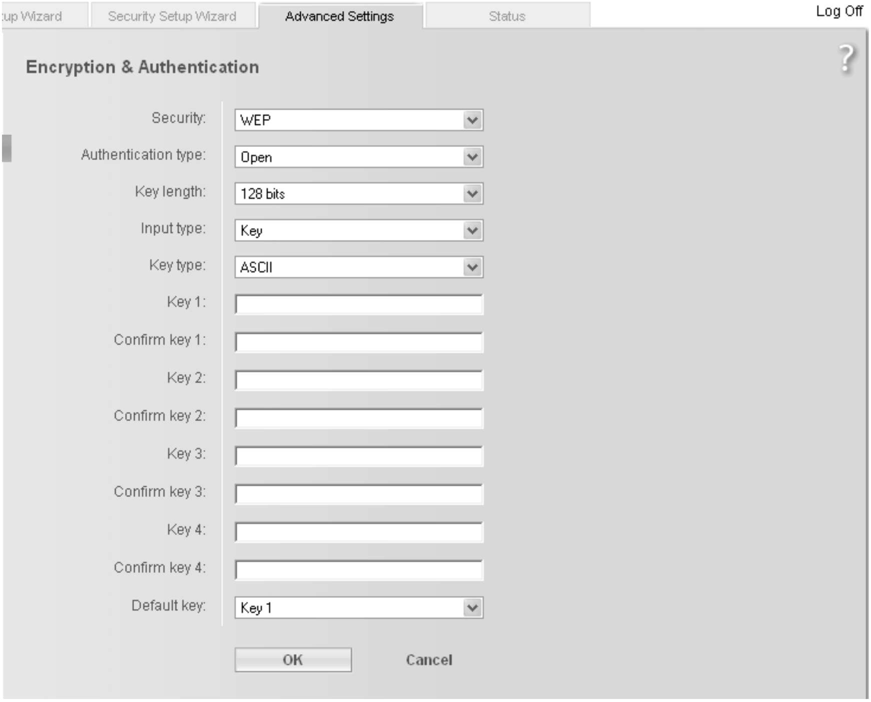
Generating the key by means of a Passphrase

→ Enter a ***Passphrase*** (up to 32 characters) and confirm it by entering it again. Four keys are generated.

→ Select one of the four keys as ***Default key***.

Manual key entry

→ Select the ***Key type***, ***Hex*** or ***ASCII***.



Encryption & Authentication

Security:	WEP
Authentication type:	Open
Key length:	128 bits
Input type:	Key
Key type:	ASCII
Key 1:	
Confirm key 1:	
Key 2:	
Confirm key 2:	
Key 3:	
Confirm key 3:	
Key 4:	
Confirm key 4:	
Default key:	Key 1

If you select ***Hex*** as the key type, you can use the characters **0** to **9** and **A** to **F**.

- With a 64-bit encryption depth the key is exactly 10 characters long.
  Example of a valid key: 1234567ABC
- With a 128-bit encryption depth the key is exactly 26 characters long.
  Example of a valid key: 234567ABC8912345DEF1234567

If you select ***ASCII*** as the key type, you can use the characters **0** to **9**, **A** to **Z**, and **a** to **z** plus the special characters in the ASCII character set.

- With a 64-bit encryption depth the key is exactly 5 characters long.
  Example of a valid key: GIGA1
- With a 128-bit encryption depth the key is exactly 13 characters long.
  Example of a valid key: GIGASET_SE336

→ Enter up to four keys in fields ***Key 1*** to ***Key 4*** and confirm these keys by entering them again in fields
Confirm key 1 to ***Confirm key 4***.

→ Select one of the four keys as ***Default key***.

Note:

◆ It is very **important** that you make a note of keys you enter or generate. You will need this information to configure the wireless network adapters correctly.

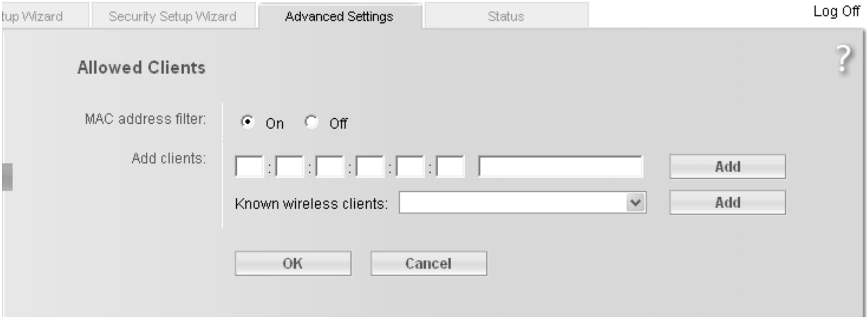
◆ When you have completed configuration you must also change WEP encryption on the wireless network adapters for the connected PCs; if you do not, they will no longer be able to access the Gigaset SE366 WLAN's wireless network.

→ Click ***OK*** to apply the settings.

Allowed clients

You can specify on this screen which PCs will have wireless access to the Gigaset SE366 WLAN and hence to your LAN.

→ In the ***Wireless Network*** menu, select ***Allowed Clients***.



Allowed Clients

MAC address filter: ● On ○ Off

Add clients: □:□:□:□:□:□ □

Known wireless clients: □

The default setting for access control is disabled. This means that all PCs that use the correct SSID can log in.

Access control is based on the MAC address of the PCs' network adapters.

→ Activate access control via the ***On*** option in the field ***MAC address filter***.

Entering PCs manually:

→ Enter the required PCs with ***MAC address*** and ***Device name*** in the appropriate fields.

→ Click ***Add*** to add the entry to the list.

→ Click ***Delete*** to delete the entry from the list.

→ Click ***OK*** to apply the settings.

Selecting from the list of known PCs

→ From the ***Known wireless clients*** list (all PCs that currently have access to the Gigaset SE366 WLAN), select the PC you want to add to the access control list.

→ Click ***Add*** to add the entry to the list.

→ Click ***OK*** to apply the settings.

Note:

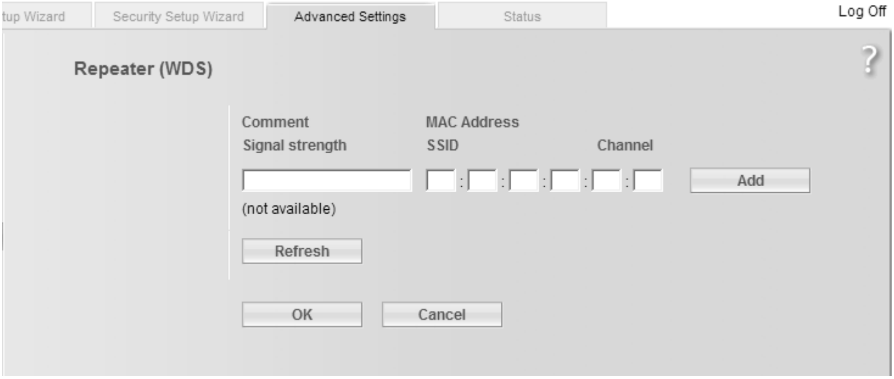
- If you have activated MAC access control and want to use WPS, please note that only clients already included in the MAC address list can register via WPS.
- If you activate MAC access control, you must at least enter the PC from which you are configuring the Gigaset SE366 WLAN. If you fail to do this, you will no longer be able to access the user interface and an error message will be shown.
- If, by mistake, you have denied all PCs access to the Gigaset SE366 WLAN you have two options:
  - You can reset the Gigaset SE366 WLAN to the factory settings (see page 20).
  - You can connect a PC to the Gigaset SE366 WLAN using one of the LAN connections (by cable). Since MAC access control only applies to PCs that are connected "wirelessly", you can use this PC to change the configuration.

Repeater function (WDS)

If you want to use a repeater in your wireless network in order to extend the range you must activate the Wireless Distribution System (WDS) function.

→ In the ***Advanced Settings*** - ***Wireless Network*** menu, choose ***Repeater (WDS)***.

All access points and repeaters in range are searched and displayed with SSID, MAC address, channel and signal strength.



→ Click ***Refresh*** to update the display.

→ Click ***Add*** to choose a device as a repeater for your wireless network.

→ Click ***Delete*** to remove a device from the list of repeaters.

→ Click ***OK*** to apply the settings.

The encryption settings on the repeater have to correspond with the settings on your Gigaset SE366 WLAN. If the repeater supports WPS, you can use WPS registration. Further information can be found in the user manual for the repeater.

If you use WPS or WPA2-PSK/WPA-PSK encryption, you can use one repeater; with WEP encryption you can use up to six repeaters via the WDS function in your wireless network.

Administration and status information

The Gigaset SE366 WLAN user interface includes several helpful functions for administration. You can

- open an Internet connection manually (see below),
- select regional options (see page 78),
- change the system password (see page 79),
- set up remote administration (see page 80),
- save, and if necessary restore, configuration data (see page 82),
- reset the Gigaset SE366 WLAN to the factory settings (see page 83),
- reboot the device (see page 83),
- update the firmware (see page 84),
- make the settings for the system protocol (see page 85),
- activate or deactivate the registration button (see page 86),
- view information about the configuration and status of the Gigaset SE366 WLAN (see page 87).

Connecting to the Internet manually

You can set up a manual connection to the Internet.

To open or close an Internet connection manually:

→ Open the Gigaset SE366 WLAN start screen as described on page 26.

If you have already started the configuration environment, click the ***Home*** tab at the top left of the window.

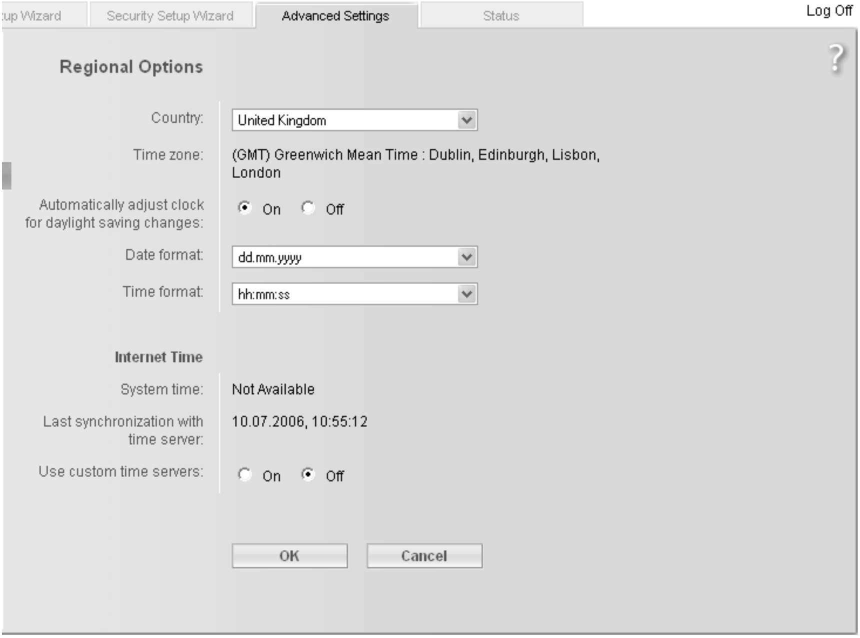
If you have not yet started the configuration environment, start it now and log in.

→ Click ***Connect*** to open a connection to the Internet.

Regional Options

To operate your Gigaset SE366 WLAN you can select the location, time zone and the format for entering the date and time, as well as configure the application for a time server for Internet time.

→ In the ***Advanced Settings*** – ***Administration*** menu, select the entry ***Regional Options***.



Regional Options

Country: United Kingdom

Time zone: (GMT) Greenwich Mean Time : Dublin, Edinburgh, Lisbon, London

Automatically adjust clock for daylight saving changes: ● On ○ Off

Date format: dd.mm.yyyy

Time format: hh:mm:ss

Internet Time

System time: Not Available

Last synchronization with time server: 10.07.2006, 10:55:12

Use custom time servers: ○ On ● Off

→ Select the country in which you are currently located from the list. You can set the clock to change automatically to summer time and/or to the ***Time zone*** as you wish.

→ Select the required option and/or select the ***Time zone*** for your location.

→ Select the required format for entering the date and time from the ***Date format*** and ***Time format*** lists respectively.

Internet Time

The ***System time*** for your device is automatically synchronised with the time server on the Internet. The time of the ***Last synchronization with time server*** is displayed for your information.

→ If you wish to use your own time server, select the ***On*** option next to the ***Use custom time servers*** field.

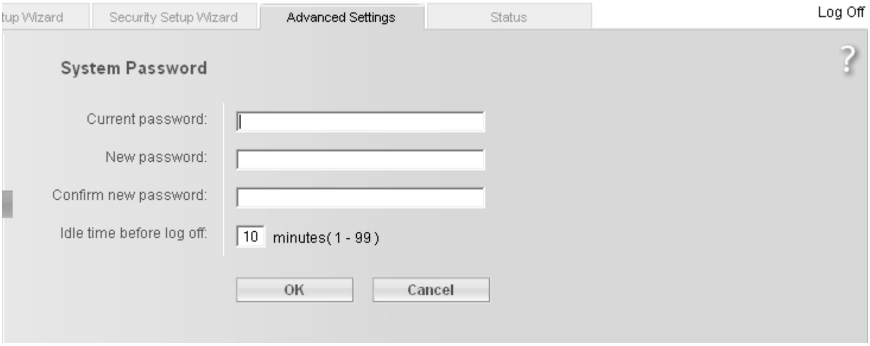
→ Enter the Internet addresses for the time servers in the ***Preferred time server*** and ***Alternate time server*** fields respectively.

→ Click ***OK*** to apply the settings.

System Password

You can assign a System Password for the configuration environment of your Gigaset SE366 WLAN and specify the period after which a session is to end automatically if no further entry is made.

→ In the ***Administration*** menu, select ***System Password***.



System Password

Current password:

New password:

Confirm new password:

Idle time before log off: 10 minutes(1 - 99)

After installation, the configuration of the Gigaset SE366 WLAN is protected by default with the System Password ***admin***. To prevent unauthorised changes to the configuration, you should set your own System Password and change it from time to time.

→ If you have already set a System Password, enter the old System Password in the ***Current password*** field.

→ Enter a new password in the ***New password*** field and repeat it in the ***Confirm new password*** field.

The password may contain up to 32 characters. The password is case sensitive. Avoid proper names and all too obvious words. Use a combination of letters, numbers and special characters.

Note:

If you ever forget your System Password you will have to reset your Gigaset SE366 WLAN (see page 21). Please bear in mind that this will restore **all** the settings to the factory configuration. The default password on delivery is ***admin***.

Setting Idle time before log off

→ Enter the period in minutes after which the configuration program is to be aborted if no entry is made. The default setting is 10 minutes.

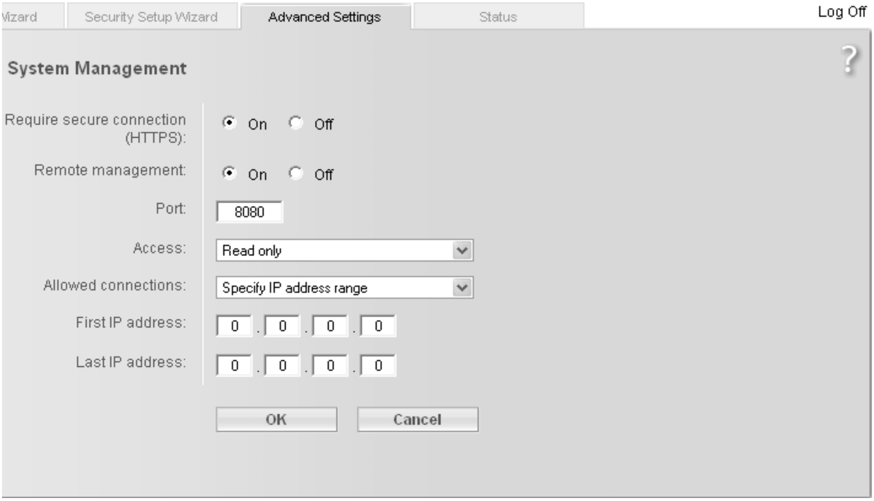
→ Click ***OK*** to apply the settings.

Setting up Remote Management

Remote Management enables a PC that is not in your local network to be used to configure the Gigaset SE366 WLAN with a standard Web browser. You can permit Remote Management for one particular PC or for any PCs.

For security reasons, this function is only available if you have previously changed the system password for your device (see page 79).

→ In the ***Administration*** menu, select ***System Management***.



System Management

Require secure connection (HTTPS): ● On ○ Off

Remote management: ● On ○ Off

Port: 8080

Access: Read only

Allowed connections: Specify IP address range

First IP address: 0 . 0 . 0 . 0

Last IP address: 0 . 0 . 0 . 0

→ ***Require secure connection (HTTPS)***

Activate this function if you want to select the secure HTTPS protocol, which an external PC can use to access the Gigaset SE366 WLAN.

If this is not the case, the HTTP protocol is used.

→ Select the ***On*** option for ***Remote Management*** if you wish to allow Remote Management.

You can start remote administration by entering the public IP address in your Internet browser. As many Internet providers change this address each time someone dials in, it is also advisable to use dynamic DNS (see page 61).

→ You can change the ***Port*** via which you access the configuration program from the Internet, for example in order to hide and protect the configuration program against unauthorised access.

→ Define ***Access (full control)*** or ***Access (read only)*** as the access right for permitted connections in the ***Access*** field.

→ ***Allowed connections:*** You can specify one particular PC or all PCs in a specific IP address block for Remote Management, or permit this function for any PCs. Select the required option from the list.

> **Note:**
>
> If you permit any PCs, then anyone who finds out your password can access this user interface and therefore also your network! If this option is needed, you should always only activate it for a short time.

Remote Management for one particular PC:

→ In the ***IP address*** field, enter the IP address of the PC that is to have access to the user interface of the Gigaset SE366 WLAN from outside your local network.

Remote Management for PCs in a specific IP address block:

→ In the ***First IP address*** and ***Last IP address*** fields, enter the IP address block of the PCs that are to have access to the user interface of the Gigaset SE366 WLAN from outside your local network.

> **Note:**
>
> - The Internet provider might assign the IP address to the PC dynamically. This can then change the IP address. Make sure that the PC that is to access the router from the Internet always has the same IP address.
> - To access the configuration environment via Remote Management, you must enter the address of the Gigaset SE366 WLAN to be maintained in the following format in the browser: **`http://X.X.X.X:8080`** (x.x.x.x stands for the IP address of the Gigaset SE366 WLAN).

→ Click ***OK*** to apply the settings.

Saving and restoring a configuration

Once you have configured your Gigaset SE366 WLAN, it is advisable to back up the settings. You can then restore them at any time, should they be accidentally deleted or overwritten.

You can also reset the configuration to the factory settings. You should always do this before passing your device on to others.

◆ In the ***Administration*** menu, select ***Save & Restore***.

Saving configuration data

→ Activate the ***Save configuration*** option.

This opens a file selection window where you can specify the file you wish to store in the backup file.

→ Select a directory on your local PC in which you wish to store the configuration file and enter a name for the file.

→ Click ***Save***.

Once the procedure has been completed, the current configuration data will have been saved to the specified file.

Restoring backups

→ Activate the ***Restore configuration*** option.

→ In your file system, select the backup file with which you wish to restore the configuration.

→ Confirm the action in the dialog screen that opens by clicking ***OK***.

→ Click ***OK***. The configuration will now be updated.

Resetting to the factory settings

You can reset the Gigaset SE366 WLAN to the factory settings. You should do this before making the device available to others or exchanging it through your dealer. If you do not, unauthorised persons will be able to use your Internet access data at your expense.

→ Select the option ***Reset configuration to factory default settings*** and click ***OK***.

→ Confirm the action in the dialogue screen that opens by clicking ***OK***.

Note:

You can restart your Gigaset SE366 WLAN if it no longer functions correctly. It should then be ready for use again (see page 20).

Please bear in mind that when the device is fully reset, **all** configuration settings will return to the factory settings. This means that you will have to completely reconfigure the Gigaset SE366 WLAN.

Reboot

You can restart your Gigaset SE366 WLAN if it no longer functions correctly. It should then be ready for use again.

→ In the ***Administration*** menu, select ***Reboot***.

→ Click ***OK*** to restart the device.

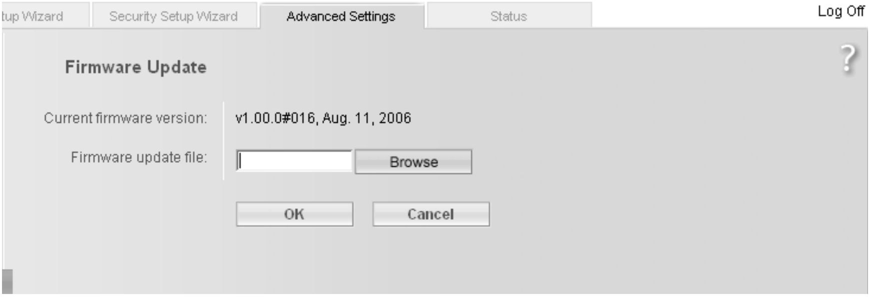
Updating the firmware

When Gigaset or your Internet provider makes a new version of the firmware available, you can update the firmware for your Gigaset SE366 WLAN. To do this you must first download the new firmware onto your PC.

Then proceed as follows:

→ Close down all network activities on your local network.

→ In the ***Administration*** menu, select ***Firmware Update***.



Firmware Update

Current firmware version: v1.00.0#016, Aug. 11, 2006

Firmware update file:

The version of the firmware currently running on your device is displayed in the line ***Current firmware version***.

→ In the ***Firmware update file*** field, enter the file with the new firmware you have downloaded from the Internet.

→ Click ***OK***.

The firmware will now be updated.

Note:
Do not switch off your Gigaset SE366 WLAN during the updating procedure. Updating can take several minutes.

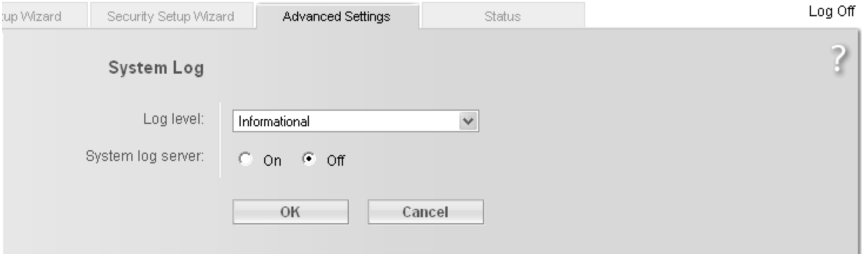
After successful updating, the device is automatically rebooted. This will take some time. After successful updating, the login screen appears again.

Note:
You can check whether the update process was successful in the ***Status*** menu on the start screen (see page 87). This displays the current firmware version running on the Gigaset SE366 WLAN.

System Log

The System Log is displayed in the ***Status*** – ***Device*** menu. It provides you with important information about the functioning of your device and potential problems. You can also have this information transmitted automatically to a system log server.

→ In the ***Administration*** menu, select ***System Log***.



Log level: Informational

System log server: ○ On ● Off

→ Make the following settings for the log:

- ***Log level***: Select how much information is to be contained in the system log. You can choose between four levels:
  - ***Critical***: logs the most important information about possible problems in your device operation
  - ***Debugging***: complete and detailed information about all your device's functions
  - ***Warning*** and ***Informational*** are intermediate levels.
- ***System log server***
  - Activate this function if you require automatic transmission of your device's system log to a system log server in your local network.
  - ***Server address***:
    Enter the IP address for the system log server.
  - ***Server port***:
    Enter the port of the system log server that is to be used to transmit the system log.

→ Click ***OK*** to accept the changes.

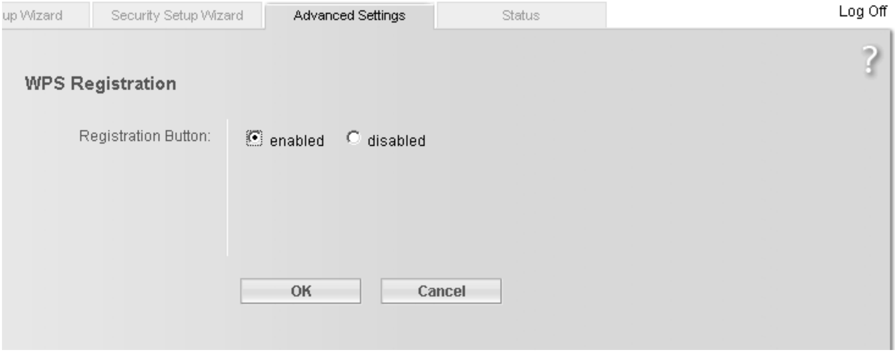
Deactivating the registration button

Your Gigaset SE366 WLAN supports WPS (see page 13) for enabling automatic configuration of the security settings in your wireless network. You can activate WPS registration via the user interface (see page 68) or via the registration button on the device's back panel (see page 20).

After finishing the configuration of your wireless network, you can deactivate the registration button for security reasons, in case unauthorised persons gain access to your Gigaset SE366 WLAN.

The registration button is activated by default.

→ In the ***Administration*** menu, choose ***Registration Button***.



WPS Registration

Registration Button: ● enabled ○ disabled

→ Select ***disabled***.

→ Click ***OK*** to accept the changes.

Status information

You can view information about the configuration and status of the Gigaset SE366 WLAN in the Gigaset SE366 WLAN's ***Status*** menu. On the first screen you will see an overview of the status of the Internet connection, the local and wireless networks, and the device.

For detailed information you can view the following status screens:

- ***Security***
- ***Internet***
- ***Local Network***
- ***Wireless Network***
- ***Device***

To display a status screen, proceed as follows:

→ Select ***Status*** on the start screen.

→ Select the entry with the information you require.

Overview

The first screen provides an overview of the current operating status and most important data for your device.

Internet

- ***Connection status***

  The status of the connection to the Internet and, if connected, the duration of the connection.

- ***IP address***

  The public IP address of your device.

Local Network

- ***IP address***

  The local IP address of your device.

- ***DHCP Server***

  The status of the DHCP server for your device and, if activated, the number of clients in your network to which IP addresses have been assigned.

Wireless Network

- ***Status***

  The status of the wireless network connection for your device and, if activated, the number of clients in your wireless network that are connected to your device.

- ***SSID***

  The identifier for your wireless network.

Device

- ***System time***

  Your device's system time.
- ***Firmware version***

  The version of the firmware currently installed in your device.

→ Click ***Refresh*** to refresh this screen and update the displayed data.

Security

You will find information about possible security risks for your device and your network in the ***Status*** menu on the ***Security*** screen.

- ***System password not changed***

  Your device's configuration program is not effectively protected against unauthorised access as you have not changed the password since setup. The section entitled "System Password" on page 79 describes how to avoid this security risk.
- ***Identification of your wireless network visible or not changed***

  Unauthorised users can also find your wireless network easily as you have not changed the ID for your wireless network (SSID) since setup and have not deactivated SSID broadcast. The section entitled "Configuration for wireless connections" on page 65 describes how to avoid this security risk.
- ***Encryption for your wireless network not activated***

  None of the data in your wireless network is encrypted when transmitted and can therefore easily be intercepted. Unauthorised users can also easily access your network, your PCs and your Internet connection by this means. The section entitled "Setting encryption" on page 69 describes how to avoid this security risk.
- ***Firewall for your Internet connection turned off***

  Your network is not protected against hackers who gain unauthorised access via the Internet. The section entitled "Firewall" on page 50 describes how to avoid this security risk.
- ***Address translation for your Internet connection turned off***

  The clients in your network are not protected against unauthorised access via the Internet. The section entitled "Setting up the NAT function" on page 56 describes how to avoid this security risk.
- ***One or more of your local clients directly exposed to the Internet***

  One or more clients in your network are directly visible to the Internet as exposed hosts and therefore particularly exposed to risk (e.g. hacker attacks). You should only activate this function where it is absolutely necessary (e.g. to operate a Web server) and where other functions (e.g. port forwarding) are not adequate. In this case you should take appropriate measures on the clients concerned. The section entitled "Opening the firewall for selected PCs (Exposed Host)" on page 60 describes how to avoid this security risk.

- ***Remote management enabled***

  Any user, including unauthorised users, who gains knowledge of the system password for your device can access your device's configuration program via the Internet. The section entitled "Setting up Remote Management" on page 80 describes how to avoid this security risk.

→ Click ***Refresh*** to refresh this screen and update the displayed data.

Internet

You will find information about the status of your device's Internet connection in the ***Status*** menu on the ***Internet*** screen.

- ***Connection status***

  Shows the status of the connection to the Internet and, if connected, the duration of the connection. If you have set ***Connect on demand*** or ***Connect manually*** as the connection mode (see page 45), you can ***Connect*** or ***Disconnect*** the connection to the Internet manually here.

- ***Connection mode***

  Shows the connection mode defined for the connection to the Internet.

- ***IP address***

  Shows the public IP address of your device.

- ***MAC address***

  Shows the public MAC address of your device.

- ***Default gateway***

  Shows the IP address of the default gateway used for the current Internet connection.

- ***Preferred DNS server***

  Shows the IP address of the preferred DNS server used for the current Internet connection.

- ***Alternate DNS server***

  Shows the IP address of the alternative DNS server used for the current Internet connection.

- ***PPPoE pass-through***

  Shows the status of PPPoE pass-through for your DSL or cable connection for establishing Internet connections straight from a PC to your network.

- ***MTU***

  MTU defines the maximum length of a data packet that can be transported over a network without fragmentation.

- ***Address Translation (NAT)***

  – ***Status***

    Shows the status of NAT (Network Address Translation) for your Internet connection.

  - ***NAT table***

    Shows the number of entries currently in the NAT table.

    Click ***Empty*** to delete all existing entries in the NAT table.

- ***Dynamic DNS***
  - ***Dynamic DNS***

    Shows the status of dynamic DNS for your Internet connection.
  - ***Domain name***

    Shows the domain name set for dynamic DNS.

→ Click ***Refresh*** to refresh this screen and update the displayed data.

Local Network

You will find information about the settings for your local network in the ***Status*** menu on the ***Local Network*** screen.

- ***IP address***

  Shows the local IP address of your device.
- ***Subnet mask***

  Shows the subnet mask used in the local network.
- ***MAC address***

  Shows the local MAC address of your device for wired data transmission.
- ***DHCP Server***
  - ***Status***

    Shows the status of the DHCP server for your device for automatic assignment of IP addresses to clients in your local network.
- ***DHCP clients***

  Shows all clients in your network that have been assigned an IP address. The ***Host name*** and the ***MAC address*** of each client are listed for identification. You are also given information about the ***IP address*** assigned to each client as well as the remaining ***Lease time*** for the IP address before the client is assigned a new address by the DHCP server.

→ Click ***Refresh*** to refresh this screen and update the displayed data.

Wireless Network

You will find information about the settings for your wireless network in the ***Status*** menu on the ***Wireless Network*** screen.

- ***Status***

  Shows the status of the connection between your device and the wireless network.
- ***SSID***

  Shows the identity of your wireless network.

- ***Channel***

  Shows the radio channel currently used for transmitting data within your wireless network.
- ***MAC address***

  Shows the local MAC address of your device for wireless data transmission.
- ***Wireless clients***

  Shows all clients in the wireless network that are currently connected to your device. The ***Host name***, the ***MAC address*** and the ***IP address*** of each client are listed for identification purposes. You will also see information about the ***Uptime*** to date of the current connection for each client in your wireless network.
- ***Repeater (WDS)***
  - ***Status***

    Shows the status of the WDS (Wireless Distribution System) used in your wireless network to increase its range.
  - ***WDS links***

    Shows the existing number of connections to other access points or repeaters in your wireless network.

→ Click ***Refresh*** to refresh this screen and update the displayed data.

Device

You will find information about the most important data for your device in the ***Status*** menu on the ***Device*** screen.

- ***System uptime***

  Shows your device's operating time since the last system start.
- ***System time***

  Shows the system time for your device.
- ***Firmware version***

  Shows the version of the firmware currently installed in your device.
- ***Bootcode version***

  Shows the version of the boot code currently installed in your device.
- ***Wireless driver version***

  Shows the version of the WLAN driver currently installed in your device.
- ***User interface version***

  Shows the version of the user interface currently installed on your device.
- ***Hardware version***

  Shows the hardware version of your device.
- ***Serial number***

  Shows the serial number of your device.

- ***System Log***

  The system log can give you important information about the functioning of your device and possible problems. You can adjust the scope of the system log to suit your needs (see the section entitled "System Log" on page 85).

➙ Click ***Refresh*** to refresh this screen and update the displayed data.

Appendix

Deactivating HTTP proxy and configuring pop-up blocker

To start the configuration program, you may need to deactivate your browser's HTTP proxy. If you use Windows Vista or Windows XP Service Pack 2, you will need to configure the popup blocker. Both procedures are described on the next pages.

Deactivating the HTTP proxy

Make sure that the HTTP proxy in your web browser is deactivated. This function must be deactivated so that your web browser can access your Gigaset SE366 WLAN's configuration pages.

The following section describes the procedure for Internet Explorer and Mozilla Firefox. First decide which browser you are using and then follow the appropriate steps.

◆ **Internet Explorer**

→ Open Internet Explorer and from the ***Tools*** menu select ***Internet Options***.

→ In the ***Internet Options*** window click the ***Connections*** tab.

→ Click ***LAN Settings***.

→ Deactivate all options in the ***LAN Settings*** window.

→ Click ***OK*** and then ***OK*** again to close the ***Internet Options*** window.

◆ **Mozilla Firefox**

→ Open Mozilla Firefox. Click ***Tools*** and then ***Settings***.

→ In the ***Settings*** window, click ***Connection Settings...***

→ In the ***Connection Settings*** window, select the option ***Direct connection to the Internet***.

→ Click ***OK*** to finish.

Configuring the popup blocker

You must allow popups for the configuration program in order to start it.

◆ **Internet Explorer**

If working with Windows XP Service Pack 2, popups are blocked by default. Carry out the following steps:

→ Right-click on the browser information bar.

→ Select ***Allow popups from this screen***.

→ Confirm the dialogue window by clicking ***OK***.

The configuration screens for the Gigaset SE366 WLAN are now allowed as popups.

You can make additional settings for popups within Internet Explorer via the ***Tools – Popup Manager*** menu item or via ***Tools – Internet Options*** on the ***Privacy*** tab.

◆ **Mozilla Firefox**

Popups are blocked by default. Carry out the following steps:

→ Open Mozilla Firefox. Click ***Tools*** and then ***Settings***.

→ In the ***Settings*** window, click the ***Web features*** tab.

→ In the ***Web Features*** window, deactivate the ***Block Popup window***.

→ Click ***OK*** to finish.

Please note:

Should you use a different popup blocker, you must configure this accordingly.

Troubleshooting

This section describes common problems and their solutions. The Gigaset SE366 WLAN is easy to monitor thanks to its LED displays. Problems can be quickly identified. If you cannot solve connection problems after checking the LED displays, please consult the other sections shown in the following table.

Symptom	Possible cause and remedial actions
Power lamp does not light up.	No power supply. ➙ Check whether the mains adapter is connected to the Gigaset SE366 WLAN and a power outlet. ➙ Check whether the power outlet and the mains adapter are working properly. If the mains adapter is not working properly, contact our customer care unit (see page 104).
The LAN LED on a connected device does not light up.	No LAN connection. ➙ Make sure that the connected device is switched on. ➙ Check whether the Ethernet cable is plugged in. ➙ Check that you are using the right cable type (CAT5) and that the cable is not too long (<100 m). ➙ Check that the network card on the connected device and the cable connections are not defective. If necessary, replace a defective network card or cable. ➙ Use the Windows device manager (***My Computer*** – ***Properties***) to check whether the network card is functioning. If you see a red cross or a question mark, then the driver may not have been installed or there is a resource conflict. Follow the Windows instructions to remedy the problem.

Symptom	Possible cause and remedial actions
You cannot connect to the Internet.	→ Check whether the ***Connect on demand*** option is deactivated. In this case, connections cannot be opened automatically. → Select ***Connect on demand***. → The connection may have been terminated manually with the ***Connect on demand*** option selected. – Open the connection again manually using the ***Connect*** button or – Restart the Gigaset SE366 WLAN. In both cases, the ***Connect on demand*** setting will be active again. → Make sure that you have entered the access data supplied by your service provider correctly. → There may be a problem at the service provider end. Get in touch with your service provider.
You cannot open a connection from a wireless device to the Gigaset SE366 WLAN.	You try to perform WPS registration on the network adapter but the registration button has not been pressed on the Gigaset SE366 WLAN. → Press the **Registration** button on the Gigaset SE366 WLAN back panel and activate WPS within two minutes on the network adapter. You defined a PIN for WPS registration but the network adapter doesn’t use any PIN or not the right one. → Check the wireless network encryption settings and find out the PIN that is used by the Gigaset SE366 WLAN. Enter this PIN on the network adapter. The wireless network adapter is not using the correct SSID. → Change the SSID on the network adapter or use the WPS function. You have set SSID and encryption manually and then performed WPS registration. → Check which SSID and pre-shared key are used and configure the WLAN clients with this data. MAC access control is activated, but the PC is not included in the MAC address list. → Enter the PC that is to register via WPS in the MAC address list.

Symptom	Possible cause and remedial actions
After a WPS registration attempt the **WLAN** LED keeps flashing and the desired client was not registered.	More than one client has tried to register. → Check if maybe an external device has registered with your network. If yes: → Change the WPA PSK key manually as soon as possible (see page 69) and perform the WPS registration via PIN (see page 68). If no: → Try to register again after a short time period.
You cannot open a connection from a wireless device to the Gigaset SE366 WLAN.	Either encryption is enabled on the Gigaset SE366 WLAN but not on the wireless network adapter, or it is not using the correct key or is using another type of encryption. → Activate the same encryption on the network adapter with the correct key or use the WPS function. If you do not know the key, you will have to reset the Gigaset SE366 WLAN (see page 20). **Warning**: Please bear in mind that this will return **all** the configuration settings to the factory settings. The ***Wireless Network*** function is deactivated. → Check whether the ***Wireless Network*** function is deactivated and, if so, activate it (see page 65). The PC does not have a wireless connection. → Use the Windows device manager (***My Computer*** – ***Properties***) to check whether the network connection is functioning. If you see a red cross or a question mark, then the driver may not have been installed or there is a resource conflict. Follow the Windows instructions to remedy the problem.

Symptom	Possible cause and remedial actions
The Gigaset SE366 WLAN or other PCs cannot be reached by a PC in the connected LAN with a **`ping`** command.	➙ Make sure that TCP/IP has been installed and configured on all the PCs on the local network. ➙ Check that the IP addresses have been correctly configured. In most cases you can use the DHCP function of the Gigaset SE366 WLAN to assign dynamic addresses to the PCs in the LAN. In this case, you must configure the TCP/IP settings of all the PCs so that they obtain their IP address automatically. If you configure the IP addresses in the LAN manually, remember to use subnet mask 255.255.255.x. This means that the first three parts of the IP address on each PC and the Gigaset SE366 WLAN must be identical. The device must also be configured as DNS server.
No connection to the Gigaset SE366 WLAN's configuration interface.	➙ Use the **`ping`** command to check whether you can establish a network connection to the Gigaset SE366 WLAN. ➙ Check the network cable between the PC you want to use to manage the device and the Gigaset SE366 WLAN. ➙ If the PC you want to use is in the router's local network, make sure that you are using the correct IP address administration (see above). ➙ If the PC you want to use is not in the router's local network, it must be authorised via Remote Management.
Password forgotten or lost	➙ Reset the Gigaset SE366 WLAN (see page 21). **Warning**: Please bear in mind that this will return **all** the configuration settings to the factory settings.
You cannot access a resource (drive or printer) on another PC.	➙ Make sure that TCP/IP has been installed and configured on all the PCs on the local network and that the PCs all belong to the same workgroup. ➙ Check whether the resource has been released on the PC in question and whether you have the necessary access rights. ➙ Printing: Check whether the printer has been set up as a network printer.

Symptom	Possible cause and remedial actions
The transmission rate is too low. For example, there are pixel errors with video streaming.	➙ Radio data transmission depends on the operating environment, for example the building stock or the influence of other devices in the vicinity that transmit in the 2.4-GHz frequency range. ➙ Arrange your WLAN devices closer together. ➙ Change the antenna direction. ➙ Position the device elsewhere. ➙ Switch off other radio sources in the vicinity. They may interfere with data transmission. ➙ Choose a different channel. ➙ Check to see if the problem also arises with a different type of encryption.

Gigaset SE366 WLAN functions and their interdependency

The following table shows which functions of your device are possible in which combination. In the case of error, check the following conditions:

Function	possible in combination with	not possible in combination with
WPS	WPA2-PSK/WPA-PSK encryption	WPA2/WPA authentication WEP encryption
IEEE 802.11n transmission mode	WPA2-PSK/WPA-PSK encryption	WPA2/WPA authentication WEP encryption
WDS	WEP encryption (up to 6 WDS connections) WPA2-PSK/WPA-PSK encryption (one WDS connection)	WPA2/WPA

Specifications

Interfaces

1 modem	RJ45, 10Base-T/100Base-TX, Autosensing, MDI/MDIX
4 LAN	RJ45, 10Base-T/100Base-TX, Autosensing, MDI/MDIX
WLAN	IEEE 802.11n (draft, see see page 15), to connect up to 32 wireless PCs

Wireless properties

Frequency range	2,400 to 2,484 GHz ISM band
Spreading	Direct Sequence Spread Spectrum (DSSS)
Modulation	CCK, OFDM
Number of channels	13: all countries except Japan, USA and Canada 11: USA and Canada
Transmission rate	IEEE 802.11b: up to 11 Mbps IEEE 802.11g: up to 54 Mbps IEEE 802.11n (draft, see see page 15): up to 300 Mbps
Range	approx. 50 m indoors, up to 300 m outdoors
Antenna design	3*3, dualband

Operating environment

Temperature	Operating temperature 0 to 40°C Storage temperature -20 to 70°C
Humidity	5% to 90% (non condensing)
LED displays	Power Online (Internet) WLAN (activity, wireless) WAN (connection to modem, activity) LAN1... LAN4 (connection to PC, activity, wired)

Compliance with security conditions and regulations

CE, EN60950
Anatel (planned)

Software	Browser-based configuration environment NAT, PPPoE DHCP server and client NAT, Port Forwarding, Port Triggering, Exposed Host Security setup Firewall, prevention of hacker attacks MAC address filtering URL filtering, DoS blocking, SPI WPA2-PSK/WPA-PSK encryption WPA2 / WPA encryption WEP encryption WPS (Wi-Fi Protected Setup) 1 click only WLAN configuration WDS

Authorisation

This device is intended for use worldwide. Use outside the European Economic Area (with the exception of Switzerland) is subject to national approval.

In France, this device is only intended for internal use within buildings.

Country-specific requirements have been taken into consideration.

We, Gigaset Communications GmbH, declare that this device meets the essential requirements and other relevant regulations laid down in Directive 1999/5/EC.

A copy of the 1999/5/EC Declaration of Conformity is available at this Internet address: www.gigaset.com/docs.

CE 0682 (!)

Approval

United Kingdom

All electrical and electronic products should be disposed of separately from the municipal waste stream via designated collection facilities appointed by the government or the local authorities.

This crossed-out wheeled bin symbol on the product means the product is covered by the European Directive 2002/96/EC.

The correct disposal and separate collection of your old appliance will help prevent potential negative consequences for the environment and human health. It is a precondition for reuse and recycling of used electrical and electronic equipment.

For more detailed information about disposal of your old appliance, please contact your local council refuse centre or the original supplier of the product.

Ireland

All electrical and electronic products should be disposed of separately from the municipal waste stream via designated collection facilities appointed by the government or the local authorities.

This crossed-out wheeled bin symbol on the product means the product is covered by the European Directive 2002/96/EC.

The correct disposal and separate collection of your old appliance will help prevent potential negative consequences for the environment and human health. It is a precondition for reuse and recycling of used electrical and electronic equipment.

For more detailed information about disposal of your old appliance, please contact your city office, waste disposal service or the shop where you purchased the product.

Service (Customer Care)

We offer you support that is fast and tailored to your specific needs!

Our Online Support on the Internet can be reached any time from anywhere.
www.gigaset.com/customercare

It provides you with 24/7 support for all our products. It also provides a list of FAQs and answers plus user guides and current software updates (if available for the product) for you to download.

You will also find frequently asked questions and answers in the appendix of this user guide.

For personal advice on our range of products and assistance with repairs or guarantee/ warranty claims you can contact us on:

UK helpdesk: 0 84 53 67 08 12.

Ireland 18 50 77 72 77.

Please have your proof of purchase ready when calling with regard to guarantee/warranty claims.

Replacement or repair services are not offered in countries where our product is not sold by authorised dealers.

Open Source Software

The Gigaset SE366 WLAN contains, among other things, Open Source Software, which is licensed under the GNU General Public License and the GNU Lesser General Public License. This Open Source Software was developed by third parties and is protected by copyright. The license texts in the original English version are provided on the next pages.

The software is made available free of charge. You are entitled to use this Open Source Software as foreseen in the above-mentioned license conditions. In the event of conflicts between these license conditions and the Gigaset Communications GmbH license conditions for the software, the above-mentioned license conditions shall prevail with respect to the Open Source Software.

The GNU General Public License (GPL) is supplied with this product. In addition, you can download the license conditions from the Internet.

- You will find the GPL on the Internet at:
  http://www.gnu.org/copyleft/gpl.html
- The source text including copyright notices of the Open Source Software can be found on the Internet at:
  http://www.gigaset.com/developer

If not already supplied with the product, you can request the source text including copyright notices from Gigaset Communications GmbH by paying a fee to cover the physical act of transferring the copy. Requests can be submitted by e-mail or fax to the address or fax number below within three years of purchase of this product, indicating the precise device type as well as the version number of the installed device software.

Kleinteileversand Bocholt

E-Mail:	kleinteileversand.com@gigaset.com
Fax:	+ 49 2871 / 91 30 29

Gigaset Communications GmbH provides no warranty for the Open Source Software contained in this product if used in any manner other than the program execution intended by Gigaset Communications GmbH. The GNU General Public License defines the warranty for defects, if any, from the author or other licensors of the Open Source Software.

Gigaset Communications GmbH specifically disclaims any warranties for defects against it if a product defect is or could have been caused by altering any Open Source Software program or the product's configuration. In addition, you have no warranty claims against Gigaset Communications GmbH in the event that the Open Source Software infringes the intellectual property rights of a third party.

Technical support shall only be provided by Gigaset Communications GmbH for the software including the Open Source Software portion contained within, if this software has not been modified.

Glossary

Access point

An access point such as the Gigaset SE366 WLAN is the central element in a wireless local area network (WLAN). It handles connection of the wireless-linked network components and regulates data traffic in the wireless network. The access point also serves as an interface to other networks, e.g. an existing Ethernet LAN or via a modem to the Internet. The network mode for wireless networks with an access point is called Infrastructure mode.

Ad-hoc mode

Ad-hoc mode describes wireless local networks (WLANs) in which the network components set up a spontaneous network without an Access point, e.g. several notebooks in a conference. All the network components are peers. They must be equipped with a wireless Network adapter.

Beacon

Beacons are data packets that are sent by devices in a wireless network to all other devices to indicate that they are available and ready to receive. Beacons are also used to synchronise the wireless network. A beacon interval is the period between two beacons in milliseconds.

Bridge

A bridge connects several network segments to form a joint network, e.g. to build a TCP/IP network. The segments can have different physical characteristics, e.g. different connections such as Ethernet and wireless LANs. Linking individual segments via bridges makes it possible to build local networks of practically unlimited size.

See also: Switch, Hub, Router, Gateway

Broadcast

A broadcast is a data packet that is not directed to a particular recipient but to all the components in a network. The Gigaset SE366 WLAN does not pass broadcast packets on to the Internet; they always remain within the local area network (LAN) administered by the Gigaset SE366 WLAN.

BSSID

Basic Service Set ID

The BSSID is used for unique differentiation between one wireless network (WLAN) and another. In Infrastructure mode the BSSID is the MAC address of the Access point. In wireless networks in Ad-hoc mode the BSSID is the MAC address of any one of the participants.

Client

A client is an application that requests a service from a server. For example, an HTTP client on a PC in a local network requests data, i.e. Web pages, from an HTTP server on the Internet. Frequently the network component (e.g. the PC) on which the client application is running is also called a client.

Connect on demand

Connect on demand means that applications such as a Web browser, Messenger and E-mail automatically open an Internet connection when they are launched. This can lead to high charges if you are not using a Flat rate. This function can be deactivated at the Gigaset SE366 WLAN to save call charges.

DHCP

Dynamic Host Configuration Protocol

DHCP handles the automatic assignment of IP addresses to network components. It was developed due to the fact that in large networks – especially the Internet – defining IP addresses is very complex as participants frequently move, drop out or new ones join. A DHCP server automatically assigns the connected network components (DHCP Clients) Dynamic IP addresses from a defined IP pool range, thus saving a great deal of configuration work. In addition, it also allows address blocks to be used more effectively: Since not all participants are in the network at the same time, the same IP address can be assigned to different network components in succession as and when required.

The Gigaset SE366 WLAN includes a DHCP server and can automatically assign IP addresses to PCs in the local network. You can specify that the IP addresses for certain PCs are never changed.

DHCP server

See DHCP

DMZ

Demilitarized Zone, see also Exposed Host

DMZ describes a part of a network that is outside the Firewall. A DMZ is set up, as it were, between a network you want to protect (e.g. a LAN) and a non-secure network (e.g. the Internet). A DMZ is useful if you want to offer Server services on the Internet which, for security reasons, will not run behind the firewall, or if Internet applications do not function correctly behind a firewall. A DMZ permits unrestricted access from the Internet to only one or a few network components, while the other network components remain secure behind the firewall.

DNS

Domain Name System

DNS permits the assignment of IP addresses to computers or Domain names, which are easier to remember. A DNS server must administer this information for each LAN with an Internet connection. As soon as a page on the Internet is called up, the browser obtains the corresponding IP address from the DNS server so that it can establish the connection.

On the Internet. the assignment of domain names to IP addresses is based on a hierarchical system. A local PC only knows the address of the local name server. This in turn knows all the addresses of the PCs in the local network and the next higher name servers, which again know addresses and the next higher name servers.

DNS server

See DNS

Domain name

The domain name is the reference to one or more Web servers on the Internet, e.g. gigaset.com. The domain name is mapped to the respective IP address via the DNS service.

DoS attack

Denial of Service

A DoS attack is a particular form of hacker attack directed at computers and networks with a connection to the Internet. The aim is not so much to steal data but to paralyse the computer or network so severely that the network resources are no longer available. A typical hacker attack involves a remote computer claiming that it is acting on behalf of a paralysed computer, for example, and receiving the data intended for you.

DSL

Digital Subscriber Line

DSL is a data transmission technology in which a connection to the Internet can be run over normal telephone lines. A DSL connection is supplied by an Internet Provider. It requires a DSL modem.

DTIM

Delivery Traffic Indication Message

A DTIM is a signal that is sent by an access point as part of a Beacon to a client device in power-saving mode to indicate that a data packet is ready for delivery. The DTIM interval defines the frequency with which a DTIM appears in a series of beacon packets.

DynDNS

Dynamic DNS

The assignment of Domain names and IP addresses is handled by the Domain Name Service (DNS). This service is now enhanced with so-called Dynamic DNS (DynDNS) for Dynamic IP addresses. This enables the use of a network component with a dynamic IP address as a Server on the Internet. DynDNS ensures that a service can always be addressed on the Internet under the same domain name regardless of the current IP address.

Dynamic IP address

A dynamic IP address is assigned to a network component automatically by DHCP. This means that the IP address of a network component can change with every login or at certain intervals.

See also Static IP address

Encryption

Encryption protects confidential information against unauthorised access. With an encryption system, data packets can be sent securely over a network. The Gigaset SE366 WLAN offers WEP encryption and WPA encryption for secure data transmission over wireless networks.

Ethernet

Ethernet is a network technology for local networks (LANs) defined by the IEEE as standard IEEE 802.3. Ethernet uses a baseband cable with a data transmission rate of 10 or 100 Mbps.

Exposed Host

Exposed Host refers to a PC outside the firewall.

See also DMZ

Firewall

Firewalls are used by network operators as protection against unauthorised external access. This involves a whole bundle of hardware and software actions and technologies that monitor and control the data flow between the private network to be protected and an unprotected network such as the Internet.

See also NAT

Flat rate

A flat rate is a special billing system for Internet connections. The Internet Provider charges a monthly fee regardless of the duration and number of logins.

Full duplex

Data transmission mode in which data can be sent and received simultaneously.

See also Half duplex

Gateway

A gateway is a device used to connect networks with completely different architectures (addressing, protocols, application interfaces, etc.). Although it is not totally correct, the term is also used as a synonym for Router.

See also Bridge, Hub, Router, Switch

Global IP address

See Public IP address

Half duplex

Operating mode for data transfer. Only one party can receive or send data at any one time.

See also Full duplex

HTTP proxy

An HTTP proxy is a Server that network components use for their Internet traffic. All requests are sent via the proxy.

Hub

A hub connects several network components in a star-topology network by sending all the data it receives from one network component to all the other network components.

See also Switch, Bridge, Router, Gateway

IEEE

Institute of Electrical and Electronics Engineers

IEEE is an international body that defines network standards, especially to standardise LAN technologies, transfer protocols, data transfer speeds and wiring.

IEEE 802.11

IEEE 802.11 is a standard for wireless LANs operating in the 2.4 GHz band. In so-called Infrastructure mode terminals can be connected to a base station (Access point) or they can connect with each other spontaneously (Ad-hoc mode).

IGMP

Internet Group Management Protocol

IGMP is an Internet Protocol that enables an Internet computer to inform neighbouring routers that it is a member of a multicast group. With multicasting, a computer can send content on the Internet to several other computers that have registered an interest in the first computer's content. Multicasting can, for example, be used for multimedia programs for media streaming to recipients that have set up multicast group membership.

Infrastructure mode

Infrastructure mode is a way of operating wireless local networks (WLANs) in which an Access point handles the data traffic. Network components cannot establish a direct connection with each other as is the case in Ad-hoc mode.

Internet

The Internet is a wide-area network (WAN) linking several million users around the world. A number of Protocols have been created for exchanging data, and these are known collectively under the name TCP/IP. All participants on the Internet can be identified by an IP address. Servers are addressed by Domain names (e.g. gigaset.com). Domain names are assigned to IP addresses by the Domain Name Service (DNS).

Among the most important Internet services are:

- electronic mail (email)
- the World Wide Web (WWW)
- file transfer (FTP)
- discussion forums (Usenet / Newsgroups)

Internet Provider

An Internet provider (Internet Service Provider) offers access to the Internet for a fee.

IP

Internet protocol

The IP Protocol is one of the TCP/IP protocols. It is responsible for addressing parties in a network using IP addresses, and routes data from the sender to the recipient. It decides the paths along which the data packets travel from the sender to the recipient in a complex network (routing).

IP address

An IP address is a network-wide unique address for a network component in a network based on the TCP/IP protocol (e.g. in a local area network (LAN) or on the Internet). The IP address has four parts (values from 0 to 255) separated by periods (e.g. 192.168.1.1). The IP address consists of the network address and the PC address. Depending on the Subnet mask, one, two or three parts form the network address, the remainder the PC address. You can find out the IP address of your PC by entering **`ipconfig`** in the command prompt.

IP addresses can be assigned manually (see Static IP address) or automatically (see Dynamic IP address).

On the Internet, Domain names are normally used instead of IP addresses. DNS is responsible for assigning domain names to IP addresses.

The Gigaset SE366 WLAN has a Private IP address and a Public IP address.

IP pool range

The Gigaset SE366 WLAN's IP address pool defines a range of IP addresses that the router's DHCP server can use to assign Dynamic IP addresses.

ISP

Internet Service Provider, see Internet Provider

LAN

Local Area Network

A local area network (or local network) links network components so that they can exchange data and share resources. The physical range is restricted to a particular area (a site). As a rule, the users and operators are identical. A local network can be connected to other local networks or a wide area network (WAN) such as the Internet.

With the Gigaset SE366 WLAN you can set up a wired local Ethernet network and a wireless IEEE 802.11g standard network (WLAN).

Lease time

The lease time defines the period for which PCs keep the Dynamic IP address assigned to them by the DHCP server without changing it.

Local IP address

See Private IP address

MAC address

Media Access Control

The MAC address is used for the globally unique identification of a Network adapter. It comprises six parts (hexadecimal numbers), e.g. 00-90-96-34-00-1A. The MAC address is assigned by the network adapter's manufacturer.

Mbps

Million bits per second

Specification of the transfer speed in a network.

MER

MAC Encapsulated Routing

Special form of transmission protocol for the Internet.

MRU

Maximum Receive Unit

The MRU defines the maximum user data volume within a data packet.

MTU

Maximum Transmission Unit

The MTU defines the maximum length of a data packet that can be carried over the network at any one time.

NAT

Network Address Translation

NAT is a method for converting IP addresses (Private IP addresses) within a network into one or more Public IP addresses on the Internet. With NAT several network components in a LAN can share the router's public IP address to connect to the Internet. The network components on the local network are hidden behind the router's IP address, which is registered on the Internet. Because of this security function, NAT is frequently used as part of a network Firewall. If you want to make services on a PC in the local network available on the Internet despite NAT, you can configure the Gigaset SE366 WLAN as a Virtual server.

Network

A network is a group of devices connected in wired or wireless mode so that they can share resources such as data and peripherals. A general distinction is made between local area networks (LANs) and wide area networks (WANs).

Network adapter

A network adapter is the hardware device that creates the connection between a network component and a local network. The connection can be wired or wireless. An Ethernet network card is an example of a wired network adapter. The Gigaset PC Card 300 and the Gigaset USB Adapter 300 are examples of wireless network adapters.

A network adapter has a unique address, the MAC address.

Public IP address

The public IP address (also known as global IP address) is a network component's address on the Internet. It is assigned by the Internet Provider. Devices that create a link from a LAN to the Internet, such as the Gigaset SE366 WLAN, have a public and a Private IP address.

Port

Data is exchanged between two applications in a network across a port. The port number addresses an application within a network component. The combination of IP address/port number uniquely identifies the recipient or sender of a data packet within a network. Some applications (e.g. Internet services such as HTTP or FTP) work with fixed port numbers; others are allocated a free port number whenever they need one.

Port Forwarding

In port forwarding the Gigaset SE366 WLAN directs data packets from the Internet that are addressed to a particular Port to the corresponding port of the appropriate network component. This enables servers within the local area network to offer services on the Internet without them needing a Public IP address.

See also: Virtual server

PPPoA

Point-to-Point Protocol over ATM

PPPoA is a Protocol that connects network components in a local Ethernet network to the Internet via an ATM network.

PPPoE

Point-to-Point Protocol over Ethernet

PPPoE is a Protocol that connects network components in a local Ethernet network to the Internet via a modem.

Private IP address

The private IP address (also known as the local IP address) is a network component's address within the local network (LAN). The network operator can assign any address he or she wants. Devices that act as a link from a local network, such as the Gigaset SE366 WLAN, have a private and a Public IP address.

Protocol

A protocol describes the agreements for communicating in a network. It contains rules for opening, managing and closing a connection, as well as about data formats, time frames and how to handle potential errors. Communication between two applications requires different protocols at different levels, e.g. the TCP/IP protocols on the Internet.

Radio network

See WLAN

RADIUS server

A RADIUS server acts as a central authentication server. In doing so, the RADIUS server handles authentication processes (user/password verification). It also provides parameters for the connection to the Client. The RADIUS server obtains the data for this function from its own configuration files, its own configuration databases or requests them from other databases or directory services that store access data (e.g. user name and password).

Rekey interval

The rekey interval is the period after which new keys are automatically generated for data encryption with WPA-PSK.

Remote management

Remote management refers to the ability to manage a network from a network component that is actually outside the local area network (LAN).

Repeater

A repeater extends the range of a wireless local area network by relaying data from the Access point to additional PCs or Network adapter.

Roaming

Roaming extends the range of a wireless LAN by using several Access points with the same SSID and the same radio channel and linked via Ethernet. The PCs in the network can switch dynamically between several access points without losing the existing network connection.

Router

A router directs data packets from one local network (LAN) to another via the fastest route. A router makes it possible to connect networks that have different network technologies. For example, it can link a local network via Ethernet or WLAN technology to the Internet.

See also Bridge, Switch, Hub, Gateway

Server

A server makes a service available to other network components (Clients). The term "server" is often used to refer to a computer or PC. However, it can also mean an application that provides a particular service such as DNS or a Web service.

SMTP

Simple Mail Transfer Protocol

The SMTP Protocol is part of the TCP/IP protocol family. It governs the exchange of electronic mail on the Internet. Your Internet Provider gives you access to an SMTP server.

SNMP

Simple Network Management Protocol

The SNMP Protocol is part of the TCP/IP protocol family. It provides a simple procedure for network administration based on a system of shared information for management data and network management messages (known as traps), and reports the occurrence of events within the monitored network (e.g. an alarm message or notification of configuration changes).

SPI

Stateful Packet Inspection

Your device uses SPI to monitor and limit access by traffic incoming from the Internet. This allows it to identify and block certain types of attack such as Denial of Service (DoS). A typical DoS attack may involve a remote computer paralysing a system and then claiming to be the paralysed device in order to receive data intended for it.

SSID

Service Set Identifier

The SSID is used to identify the stations in a wireless network (WLAN). All wireless network components with the same SSID form a common network. The SSID can be assigned by the network operator.

Static IP address

A static IP address is assigned to a network component manually during network configuration. Unlike a Dynamic IP address, a static IP address never changes.

Subnet

A subnet divides a network into smaller units.

Subnet mask

The subnet mask determines how many parts of a network's IP address represent the network address and how many parts represent the PC address.

The subnet mask in a network administered by the Gigaset SE366 WLAN is always 255.255.255.0. This means that the first three parts of the IP address form the network address and only the final part is used for the PC address. In this case, the first three parts of the IP address of all network components are therefore always the same.

Switch

Like a Hub, a switch is an element used to link different network segments or components. Unlike a hub, however, a switch has its own intelligence, which enables it to forward packets only to the subnet or network component for which they are intended.

See also Bridge, Hub, Router, Gateway

TCP

Transmission Control Protocol

The TCP Protocol is part of the TCP/IP protocol family. TCP handles data transport between communication partners (applications). TCP is a session-based transmission protocol, i.e. it sets up, monitors and terminates a connection for transporting data.

See also UDP

TCP/IP

Protocol family on which the Internet is based. IP forms the basis for every computer-to-computer connection. TCP provides applications with a reliable transmission link in the form of a continuous data stream. TCP/IP is the basis on which services such as WWW, Mail and News are built. There are other protocols as well.

TKIP

The Temporal Key Integrity Protocol (TKIP) is part of the IEEE 802.11i standard and is used to encrypt data in wireless networks.

UDP

User Datagram Protocol

UDP is a Protocol from the TCP/IP protocol family, which handles data transport between two communication partners (applications). Unlike TCP, UDP is a non-session based protocol. It does not establish a static connection. The data packets, so-called datagrams, are sent as a Broadcast. The recipient alone is responsible for making sure the data is received. The sender is not notified about whether or not it is received.

UPnP

Universal Plug & Play

UPnP technology is used to spontaneously link home or small office networks. Devices that support UPnP carry out their network configuration automatically once they are connected to a network. They also provide their own services or use services of other devices on the network automatically.

URL

Universal Resource Locator

Globally unique address of a domain on the Internet.

Virtual server

A virtual Server provides a service on the Internet that runs on another network component, not on the server itself. The Gigaset SE366 WLAN can be configured as a virtual server. It will then direct incoming calls for a service via Port Forwarding directly to the appropriate Port of the network component in the local network.

WAN

Wide Area Network

A WAN is a wide area network, which is not restricted to one particular area. The Internet is the most frequently used WAN. A WAN is run by one or more public providers to enable private access. You access the Internet via an Internet Provider.

WEP

Wired Equivalent Privacy

WEP is a security protocol defined in the IEEE 802.11 standard. It is used to protect wireless transmissions in a WLAN against unauthorised access with Encryption of the data transmitted.

WLAN

Wireless LAN

Wireless LANs enable network components to communicate with a network using radio waves as the transport medium. A wireless LAN can be connected as an extension to an existing wired LAN or it can form the basis for a new network. The basic element of a wireless network is the radio cell. This is the area in which wireless communication takes place. A WLAN can be operated in Ad-hoc mode or Infrastructure mode.

WLAN is currently specified in the IEEE 802.11 standard. The Gigaset SE366 WLAN hardware complies with standard 802.11n (draft). A software update will be provided when the standard is passed.

WPA

WPA was developed to improve the security provided by WEP. WPA uses more complex procedures to generate keys, e.g. TKIP (Temporal Key Integrity Protocol). In addition, WPA can use an authentication server (e.g. a RADIUS server) to improve security.

WPA-PSK

WPA Pre-shared Key

Variant of WPA data encryption in which new keys are generated automatically at regular intervals by means of a keyword (pre-shared key). The key is updated at defined intervals (Rekey interval).

WPS

WiFi Protected Setup

WPS simplifies the setting up of wireless networks.

WPS automatically sets up secure wireless network. Access points automatically generate a network ID (SSID) and WPA-PSK Encryption automatically. Clients can be connected either by entering a PIN or using special registration buttons on the access point and client.

Index

Issued by
Gigaset Communications GmbH
Schlavenhorst 66, D-46395 Bocholt

www.gigaset.com

A31008-M1063-R101-4x-7619